Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive“-Verfahrens (V 0.10)

Autoren: S. Gonscherowski, T. Herber, R. Robrahn[1], M. Rost, R. Weichelt
Kontakt: Martin Rost, uld32@datenschutzzentrum.de

Inhalt

[1] Die Mitwirkung an der vorliegenden Datenschutz-Folgenabschätzung der Autoren Gonscherowski, Herber und Robrahn erfolgte im Rahmen von Forschungsprojekten, die mit Mitteln des Bundesministeriums für Bildung, und Forschung unter den Förderkennzeichen 16KIS0355 (VVV), 16 KIS0424 (PARADISE) sowie 16KIS0434 (SeDaFa) gefördert wurden. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Teil A – Klärung des Zwecks des „Planspiels“

Entlang eines mit knapp zwei Seiten Text umrissenen Fall-Beispiels (siehe im Anhang auf S. 56) soll eine Datenschutzfolgeabschätzung (DSFA) durchgeführt werden. Im Rollenverständnis der Autoren der vorliegenden DSFA wird das Agieren einer Projektgruppe des Verantwortlichen („Insight AG“) simuliert, die eine DSFA nach Art. 35 Abs. 1 DSGVO, unter Rückgriff auf die Methodik des SDM, im Auftrag des Verantwortlichen – der Versicherung „Insight AG“ – durchführt. Kommentare methodischer oder rechtlicher Art, die im Text eingestreut sind, sowie das Kapitel der rechtliche Beurteilung stammen vom Datenschutzbeauftragten der Insight AG, der der Projektgruppe beratend zur Seite steht.

Anhand der Erarbeitungen zweier Datenschutzfolgenabschätzungen soll ein Vergleich zwischen der Methode nach dem Standard-Datenschutzmodell[2] (SDM), die für diesen Text verwendet wurde, und nach ISO 29134, unter Rückgriff auf den Maßnahmenkatalog der französischen Datenschutzaufsichtsbehörde CNIL durchgeführt werden, die das LDA Bayern vorstellt.

Die Nutzung des SDM zur Bestimmung des Zuschnitts von Funktionen und Schutzmaßnahmen des operativen Datenschutzes eines Verfahrens setzt die Klärung der Rechtsgrundlage und der rechtlichen Anforderungen voraus, die im Modellfall nicht angesprochen wurden.

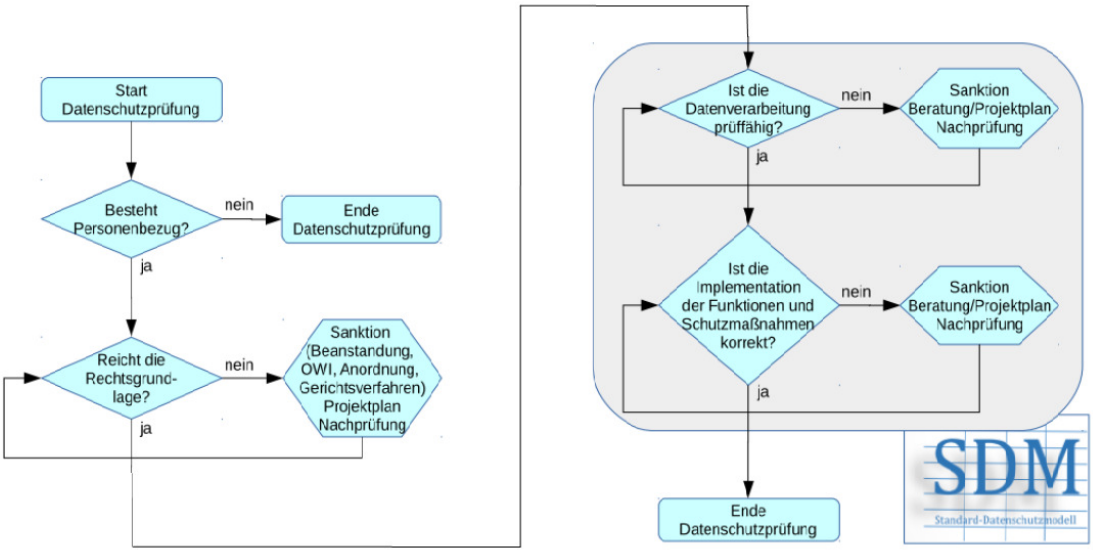


Abbildung 1: Ablaufmodell einer Prüfung/Beratung mit SDM

Die Klärung der Rechtsgrundlagen und der vom Verfahren zu erfüllenden Anforderungen ist eine Voraussetzung zur Anwendung des SDM und ebenso ein notwendig zu durchlaufender Prozessschritt des DSFA-Frameworks, das für die vorliegende DSFA genutzt wird und als „FP-Prozessmodell“ be-

[2] Datenschutzbeauftragtenkonferenz 2016: Handbuch zur SDM-Methodik, V1.0 https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf

zeichnet wird. Dieses Framework zur Durchführung einer DSFA ist dem „Whitepaper Datenschutz-Folgenabschätzung“[3] und dem Aufsatz von Bieker et al.[4] entnommen.[5] Beide Frameworks nutzen für die Risikoabschätzung und die Bestimmung der Maßnahmen explizit das SDM. In der Unterarbeitsgruppe SDM („UAGSDM“) wurde aus beiden Texten heraus ein interner, noch nicht abgestimmter und deshalb auch unveröffentlichter Arbeitsentwurf für eine „Orientierungshilfe zur Datenschutz-Folgenabschätzung“ erstellt, der wiederum die Grundlage für die nachfolgende Strukturierung der vorliegenden DSFA bildet.

[3] Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt: Michael Friedewald, Hannah Obersteller, Maxi Nebel, Felix Bieker, Martin Rost, 2016: White Paper - Datenschutz-Folgenabschätzung, ein Werkzeug für einen besseren Datenschutz, 2. Auflage, Mai 2016 http://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf

[4] Bieker, F. / Hansen, M. / Friedewald, M., 2016/09: Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung; in: RDV (Recht der Datenverarbeitung), Heft 4, 188-197

[5] Das DSFA-Prozessmodell des Whitepapers wurde aus der Synthetisierung verschiedener PIA-Ablaufmodelle entwickelt, während in dem Aufsatz dieses Modell speziell auf die Anforderungen der DSGVO abgestimmt wurde. Siehe die PIA-Modelle der CNIL (Commission Nationale de l’Informatique et des Libertés) (2015). Privacy Impact Assessment: Methodology (how to carry out a PIA). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf (10.03.2016) sowie aus dem englischen Sprachraum: Warren, A.; Charlesworth, A. (2012): Privacy Impact Assessment in the UK. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 205-224.

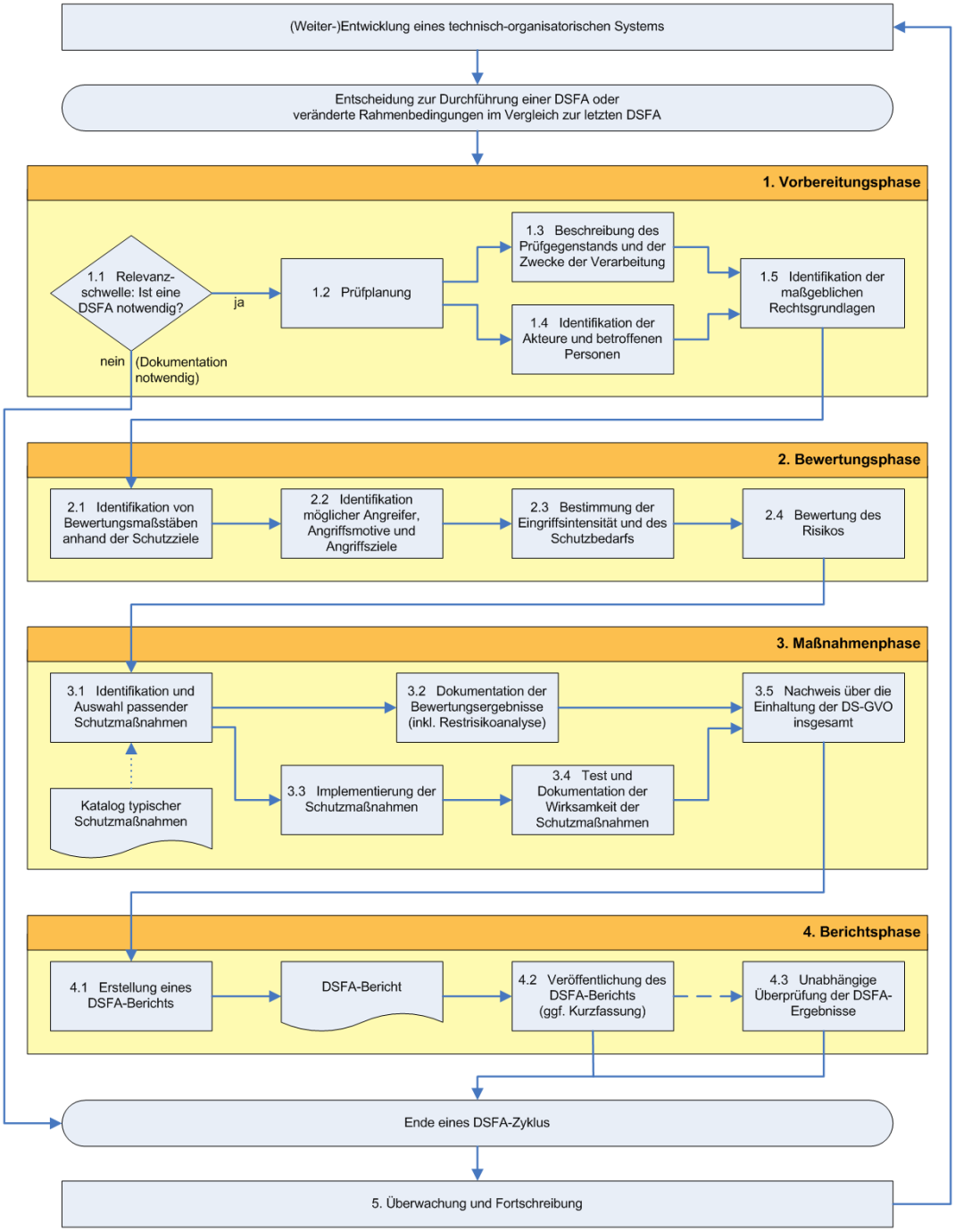


Abbildung 2: DPIA-Ablaufmodell („FP-Modell“, aus: Bieker/Hansen/Friedewald 2016)

Teil B – Erarbeiten einer DSFA mit SDM-Bezug

Das Schema des hier genutzten FP-Ablaufmodells umfasst vier aufeinander abgestimmte Phasen:

- Vorbereitungsphase
- Bewertungsphase
- Maßnahmenphase
- Berichtsphase

In der Vorbereitungsphase (1) ist zunächst das geplante Verfahren sowie der rechtliche und operative Kontext der Datenverarbeitung zu beschreiben, der anschließend in der Bewertungsphase (2) aus der für den Datenschutz zentralen Risiko-Perspektive der Betroffenen zu beurteilen ist. Sodann werden in der Maßnahmenphase (3) Vorkehrungen beschrieben, die zu treffen sind, um die identifizierten Risiken einzudämmen. Schließlich werden in der Berichtsphase (4) die Ergebnisse des DSFA-Verfahrens dokumentiert.

1. Vorbereitung

In diesem Kapitel wird die Entscheidung darüber, dass eine DSFA durchzuführen ist, knapp begründet. Es folgen Ausführungen zur Planung der Durchführung der DSFA, es wird der zu prüfende Gegenstand, also das personenbezogene Verfahren genauer beschrieben und so die DSFA fokussiert. Für die Prüfung eines Verfahrens ist es notwendig, dieses abzugrenzen in Bezug auf Datenbestände, IT-Systeme und Prozesse, weil ein Verfahren zumeist auf Bestandteile anderer Verfahren und deren Daten, IT-Systeme und Prozesse angewiesen ist, die zudem oftmals von anderen Organisationen zu verantworten sind. Inhaltlich wesentlich sind dann die Identifikation der unmittelbar beteiligten Akteure und die Sichtung der für das Verfahren relevanten Rechtsgrundlagen.

1.1 Relevanzschwelle

Eine DSFA ist durchzuführen, weil in dem Verfahren ein Scoring menschlichen Verhaltens zum Einsatz kommt (gem. Art. 35, Abs. 3a DSGVO).

1.2 Prüfplanung

Der Verantwortliche hat die DSFA durchzuführen.

Für den Modellfall nehmen wir an, dass der für die Durchführung Verantwortliche einen Projektmanager beauftragt hat die DSFA zu planen, mit Hilfe eines interdisziplinär zusammengesetzten Teams durchzuführen und dabei die Ratschläge eines Datenschutzbeauftragten (DSB) einzuholen.

Das SDM empfiehlt für die Planung von Verfahren mit hohem Schutzbedarf als *good practice* die Nutzung einer Projektmanagementmethode, um sicherzustellen, dass sämtliche relevanten Akteure ihre Interessen in das Projekt einbringen können und kein wichtiger Aspekt übersehen wird. Eine etablierte Projektmanagementmethode sichert die Klärung des Projektauftrags und nutzt die Instrumente eines Lasten- und Pflichtenhefts, was von Beginn an zur Klärung einer legitimen Zwecksetzung, angemessenen Zwecktrennung und engen Zweckbindung beiträgt.

1.3 Beschreibung des Prüfgegenstands und der Zwecke der Verarbeitung

Das Verfahren sieht vor, Handlungen eines Fahrers aus technischen Daten eines Kraftfahrzeug (Kfz) abzuleiten und zu einem Punktwert (Score) zusammenzustellen. Der Score, der als Maß für die Risikobereitschaft eines Fahrers steht, soll Einfluss auf die Festsetzung der Versicherungsprämie haben gemäß des Zusammenhangs: Eine nachgewiesen gute Fahrweise führt zu einer Teilerstattung der Versicherungsprämie. Unklar ist, ob die Einstufung von Kfz-Haltern als „wenig-riskant“, „durchschnittlich riskant“ oder „erhöht riskant“ oder mit anderen Abstufungen, z.B. anhand des Kundendatenbestands der Versicherung erfolgt. Insofern liegt ein zweifellos personenbezogenes Verfahren vor.

Darüber hinaus sollen Daten in einer anonymisierten Form zur Fortentwicklung des Scoring-Algorithmus sowie zur Unfallforschung zur Verfügung gestellt werden.

Der Prüfgegenstand (Target of Evaluation (ToE)) ist das personenbezogene Verfahren – mit den personenbezogenen Daten, den zur Erhebung und Verarbeitung herangezogenen IT-Systemen und den Prozessen – mit dem der Score eines Kfz-Halters, anhand von im Kfz erhobenen Fahreigenschaften, öffentlich zugänglichen Informationen und durch arbeitsteilige Beteiligung mehrerer Dienstleister errechnet wird. Für den Anwendungsfall gehen wir davon aus, dass die Kfz-Daten ohnehin im Fahr-

zeug erzeugt und gespeichert werden.[6] Das zu prüfende Verfahren, der Prüfgegenstand, dieser DSFA beginnt ab der OBD2-Schnittstelle (Kurzform für „On-Board-Diagnose der 2. Generation"-Schnittstelle). Die ganz wesentliche Hauptproblematik dieses Verfahrens, und zwar auf welcher Rechtsgrundlage diese Eigenschaften des Kfz erhoben werden, bleibt unbeachtet. Welche Kfz-Daten die verschiedenen Kfz-Hersteller erheben, wie groß die Speicher für diese Daten sind, für welche Zeiträume sie gespeichert werden und ob sie gelöscht werden können, ist unbekannt bzw. von Hersteller zu Hersteller verschieden.[7] Hier gilt im Grundsatz: Je neuer das Kfz, desto größer ist der Speicher für technische Daten, und desto mehr personenbezogene Daten werden erhoben.

[6] Darunter fallen sowohl die erstmalig gespeicherten als auch die erhobenen Daten. Das bedeutet auch, dass der gesamte Erhebungszusammenhang im Kfz durch die Sensorik für diesen ToE unberücksichtigt bleibt.

[7] https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx?ComponentId=260789&SourcePageId=8749&quer=daten; zuletzt angesehen am 21.06.2017.

Schematische Darstellung des ToE gemäß Sachverhalt

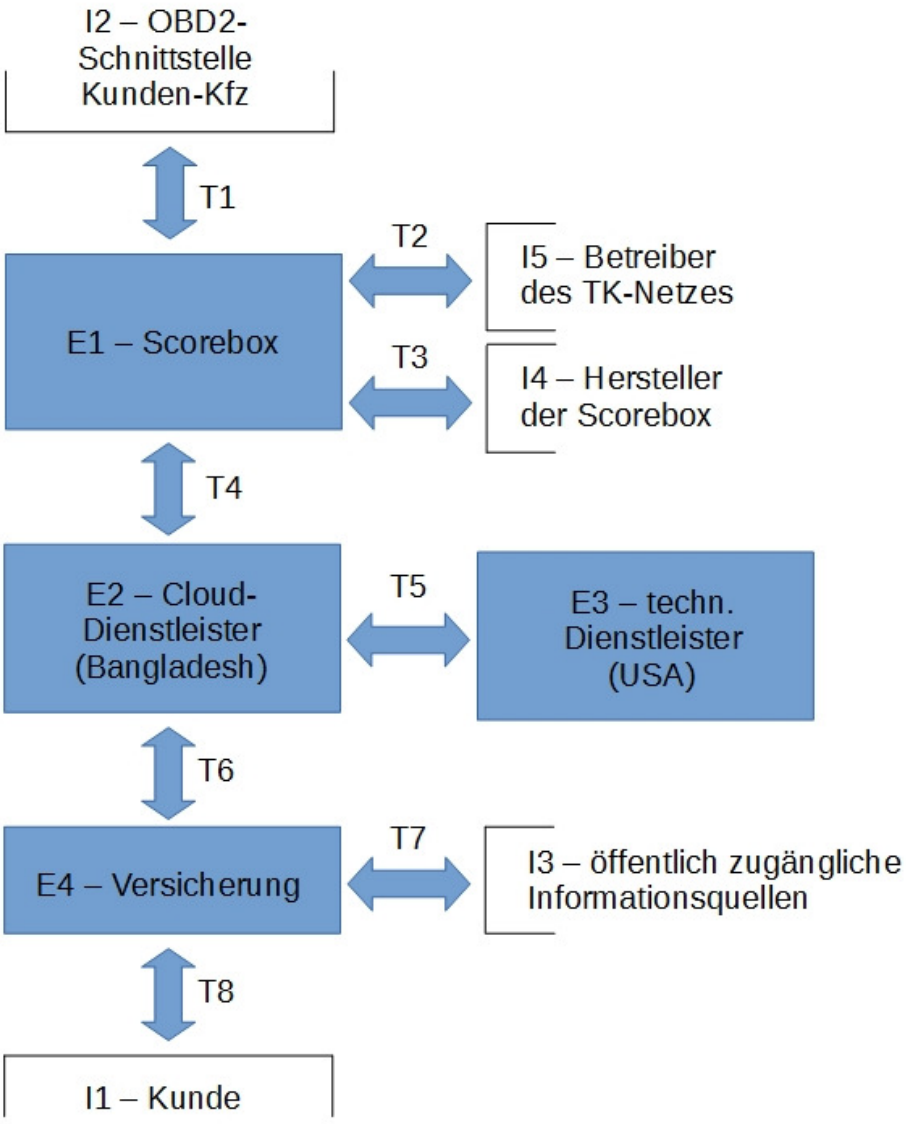


Abbildung 3: Datenflussdiagramm des Modellfalls

Zeichenerklärung:	
?	nicht angegeben

Subsysteme/Beteiligte (E1 - E5)	**verarbeitete Daten**	**Zweck**	**Rechtsgrundlage**	**Speicherdauer**	**Sicherheitsmaßnahmen**
E1 – Scorebox	Datenpaket 1	Telematik-Versicherungstarif	Vertrag	?	?
E2 – Cloud-Dienstleister (Bangladesh)	Datenpaket 1	Telematik-Versicherungstarif	?	?, mindestens 1 Jahr anzunehmen	?
E3 – techn. Dienstleister (USA)	mindestens Datenpaket 1 (für die Backups), sonst ?	Support, Backup für Dienstleister E2	EU-Standardvertrag	?	?
E4 – Versicherung (Insight AG)	Datenpakete 1 und 2	Telematik-Versicherungstarif	Versicherungsvertrag	3 Jahre vollständig incl. Fahrgestellnummer, ohne diese Nummer unbegrenzt	?

Tabelle 1: Zusammenstellung der im Modellfall aufgeführten Komponenten

Datenpaket 1	**Datenpaket 2**
Fahrgestellnummer GPS-Position mit einer Genauigkeit von 1 bis 3 Metern Höhe Beschleunigungswerte Uhrzeit Motordrehzahl, Drosselklappenstellung, Motortemperatur, Motorlast Batteriespannung	Fahrtroute, Geschwindigkeit, Verlangsamung/Bremsen vor Abzweigungen/Kreuzungen, Beschleunigung nach Abzweigungen/Kreuzungen Bremsen vor Kurven, Bremsen auf gerader Strecke, Beschleunigung auf gerader Strecke, Anzahl der über die App aufgezeichneten gefah-

Merkmale des Kfz (Marke, Modell, Baujahr) Sitzposition Güte der Bremsbeläge Servicemeldungen wie z.B. Ölfüllstand, Wartung, Glühlampe defekt	renen Kilometer, Anzahl der über die App aufgezeichneten Fahrten, Geschwindigkeitsbegrenzungen auf den Fahrtstrecken, Straßentypen (Autobahn, Bundes-, Landes- oder Ortsstraße), Einwohnerdichte in der Umgebung der Fahrtstrecken, Uhrzeit und Wochentag, Anzahl Kneipenbesuche, Anzahl Straßenrennen mit anderen Telematik-Versicherten, vermutete Geschlecht des Fahrers/der Fahrerin u vermutete ethnische Herkunft des Fahrers/der Fahrerin

Tabelle 2: Die Daten, die im Modellfall an der OBD2-Schnittstelle erhoben werden sollen

Schnittstellen (I1 – I4)	**Daten**	**Sicherheitseigenschaften**
I1 – Mitteilungen an die Kundschaft	Höhe des Rabatts	(nicht zutreffend)
I2 – OBD2-Schnittstelle des versicherten Fahrzeugs	Datenpaket 1 und weitere z.B. zur Funktion der Abgasreinigungssystems, Ansprechen von ABS, Gurtstraffern und anderen Sicherheitseinrichtungen	Lesezugriff auf alle Daten, teilweise auch Schreibzugriff; teilweise Authentifikation erforderlich
I3 – öffentlich zugängliche Informationen	?, mindestens: georeferenzierte Daten über das Straßennetz incl. Straßentypen, Geschwindigkeitsbegrenzungen, Höhen, Kurvenradien, Einwohnerdichten, Orte von Gaststätten	?
I4 – Hersteller der Scorebox	Software der Scorebox, evtl. Zugangsdaten zur Scorebox	?

I5 – Betreiber des TK-Netzes	Stammdaten, Verkehrsdaten zumindest individuell pro Scorebox	(nicht relevant)

Tabelle 3: Die Schnittstellen der Komponenten, die darüber zugänglichen Daten und etwaige Sicherheitseigenschaften

Verbindungen (T1 - T7)	**übertragene Daten (rechtliche Grundlagen: siehe die Beteiligten)**	**Übertragungsfrequenz**	**Sicherheitsmaßnahmen**
T1 – Übertragung zwischen OBD2-Schnittstelle und Scorebox	Datenpaket 1	sekündlich	drahtgebundene Übertragung; Scorebox und OBD2-Schnittstelle im Fahrgastraum verschlossen
T2 – Übertragung zwischen Scorebox und Telekommunikationsunternehmen	Metadaten zu den von der Scorebox aufgebauten Verbindungen	?, dauernd während des Fahrzeugbetriebs	abhängig vom verwendeten Mobilfunk-Protokoll
T3 – Übertragung von Daten zwischen Scorebox und Hersteller	bei Fernwartung evtl. in der Scorebox gespeicherte Nutz- und Log-Daten, sonst Updates für die Scorebox-Software	?, nach Bedarf	?
T4 – Übertragung zwischen Scorebox und Cloud-Dienstleister	Datenpaket 1, Metadaten zur Durchführung dieser Übertragungen	?, dauernd während des Fahrzeugbetriebs	Daten werden zur Übertragung mit selbst entwickeltem Algorithmus verschlüsselt und mittels Mobilfunk und ab dem DE-CIX-Knoten per Internet ohne weitere Sicherungsmaßnahmen übermittelt
T5 – Übertragung zwischen Cloud-Dienstleister und techn. Dienstleister	Backups des Datenpakets 1, nicht spezifizierte Daten im Rahmen der Wartung, Metadaten zur Durchführung dieser Übertragungen	?	?
T6 – Übertragung zwischen Cloud-	Backups des Datenpakets 1, Metadaten zur	?, mindestens ein-	?

Dienstleister und Versicherung	Durchführung dieser Übertragungen	mal jährlich	
T7 – Übertragung der Daten zwischen Versicherung und Anbietern von öffentlich zugänglichen Informationsquellen	mindestens: georeferenzierte Daten über das Straßennetz incl. Straßentypen, Geschwindigkeitsbegrenzungen, Höhen, Kurvenradien, Einwohnerdichten, Orte von Gaststätten, Metadaten zur Durchführung dieser Übertragungen (unklar, ob diese Daten einzelfallbezogen oder als Gesamtpaket von den Anbietern geladen werden)	?, mindestens einmal jährlich	?
T8 – Übertragung von Versicherung zur Kundschaft, soweit für das ToE relevant	Höhe des Rabatts	einmal jährlich	?

Tabelle 4: Die Eigenschaften zwischen den Verbindungen der Komponenten

Es ist damit zu rechnen, dass weitere Schnittstellen, sowohl von den Herstellern als auch von der Versicherung vorgesehen sein können. Damit sind weitere Datenschutz- und IT-Sicherheitsrisiken verbunden, die hier aber nicht weiter betrachtet werden, weil sie außerhalb des ToE liegen.

Die verwendete Schnittstelle OBD2 ist für alle Fahrzeuge, die seit 1996 für die USA, und für Ottomotoren, die für die EU seit 2001 gebaut wurden, aufgrund rechtlicher Verpflichtungen eingebaut. In erster Linie dient sie zur Überprüfung der Einhaltung von Abgaswerten der Fahrzeuge. Die Schnittstelle ermöglicht jedoch ein Auslesen verschiedener Fahrzeugdaten, wie beispielsweise Tankfüllung, Motordrehzahl, Fehlermeldungen, gefahrene Kilometer, Umgebungstemperatur, Zeit seit Motorstart und Gaspedalstellung. Die Schnittstelle kann jederzeit ausgelesen werden.[8] Es gibt keinerlei Zugriffsbeschränkungen und Lesegeräte sind schon für wenige Euro erhältlich.

1.4 Identifikation der mit dem Verfahren befassten unmittelbaren Akteure

Es folgt eine Auflistung derjenigen Akteure, die entweder in einer Rechtsbeziehung zueinander stehen oder die unmittelbar gestaltenden Einfluss auf das Verfahren nehmen können. Dazu zählen:

a) Die **Versicherung**, als Hersteller und Betreiber des Verfahrens

[8] https://www.obd-2.de/obd-2-allgemeine-infos.html; zuletzt abgerufen am 21.06.2017.

- Mitarbeiter der Versicherung, u.a. Sachbearbeitung, nach Sachgebieten getrennt, Kundenbetreuung, Mathematiker, Gutachter, etc. (die Beschreibung macht dazu keine Angaben)
- Leitung
- Administration mit verschiedene Zuständigkeiten
- Controlling (Finanzbuchhaltung, betrieblicher Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Betriebsrat)
- eventuell andere Bestandteile einer Versicherungsholding

b) der versicherte **Kfz-Halter** und vermutlich überwiegende Fahrer, evtl. weitere Fahrer des Kfz sowie **Mitfahrer**. Auch Mitfahrern kann über eine App die Route des Kfz zugerechnet werden. Mitfahrer tragen zur Erhöhung des Gesamtgewichts des Kfz bei. Durch Sensoren im Sitz (Sitzposition) ist eine Identifikation anderer Fahrer möglich und zumindest identifizierbar.

c) Akteure rund um das Kfz

- **Kfz-Hersteller**, mit Kfz-Bestandteilen, bei denen mittels Sensoren Daten über Zustände erhoben und gespeichert werden
- **Kfz-Werkstätten**, die die Technik zur Kfz-Überwachung installieren, die die Daten möglicherweise auch auslesen und möglicherweise auch ändern können (herstellerspezifisch, herstellerunspezifisch)

d) der **Cloud-Betreiber** zum Zwischenspeichern der Kfz-Daten sowie möglicherweise auch zur Errechnung der Aktivitäts-Scores in Bangladesch. Hier sind zwei Dienstleistungen zu unterscheiden, wobei in dem Modellfall nicht hinreichend klar klargestellt ist was zutrifft:

a) Kommunikation und Speichern, die Versicherung erzeugt dann die Fahrverhaltens-Score.
b) Zusätzlich könnte vom Cloud-Betreiber auch die Weiterverarbeitung (Verdichtung, Erzeugung von Scores) durchgeführt werden.

Wir legen den Modellfall im Sinne von a) aus, nämlich dass die Errechnung des Fahrverhaltenscores nicht durch den Cloud-Betreiber, sondern durch die Versicherung intern durchgeführt wird.

e) ein weiterer **Cloud-Betreiber** als Backup- und Wartungsservice für die oben genannte Cloud in den USA

f) der **Telekommunikationsprovider** für die Übertragung der Daten vom Kfz in die Cloud

g) der **Hersteller** der Scorebox inkl. des Funk-Tools im Kfz

Zwischen all diesen am Verfahren Beteiligten sind seitens der Versicherung als Verfahrensverantwortlichem Verträge vorzusehen, die datenschutzrechtliche Bestandteile zur Ermächtigung der Datenverarbeitung (Erhebung der Daten an der OBD2-Schnittstelle, Berechnungen, Übertragung, Löschung/Archivierung) und die Zusicherung von Schutzmaßnahmen ausweisen müssen.

Als weiterer Beteiligter kämen noch die Organisationen infrage, von denen die öffentlich verfügbaren Informationen – das Kartenmaterial zum Beispiel – bezogen werden. Unklar ist, was hier „öffentliche Verfügbarkeit“ bedeuten soll, wenn bspw. OpenStreetMap die kommerzielle Nutzung ihres Materials verbietet. Wenn anstatt öffentlichen Kartenmaterials ein kommerzieller „Kartenprovider“ genutzt

würde, würden dadurch vermutlich weitere Aspekte der Lokalisation von Standorten durch Dritte zu beachten sein.

Bewertungskriterien des Risikos

Zur genaueren Bestimmung der einer natürlichen Person entstehenden konkreten Schäden können Aspekte, wie bspw. die in Erwägungsgrund 75 genannten, als Bewertungskriterien für Risiken herangezogen werden:

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanziellen Verlust,
- Rufschädigung,
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- unbefugte Aufhebung der Pseudonymisierung oder
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

Auch für den Fall, dass keiner dieser Aspekte, die aus dem Katalog von Risiken aus dem Kontext der IT-Sicherheit stammen, zutrifft bedeutet das nicht, dass deshalb kein Datenschutzrisiko besteht. Der Erwägungsgrund 75 führt neben diesem Katalog aus,

"Die Risiken für die Rechte und Freiheiten natürlicher Personen (...) können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere (...) wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft (...) hervorgehen, (...) wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, (...) oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft."

Allein der Umstand, dass die Aufenthaltsorte oder Ortswechsel einer Person durch eine Organisation nicht nur theoretisch sondern, wie im vorliegenden Fall, tatsächlich im Sekundentakt beobachtet werden, bestimmt das für den Datenschutz wesentliche Risiko für die Rechte und Freiheiten einer Person.

Im Erwägungsgrund 76 wird die Schwere des Risikos wie folgt bestimmt: *„Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen soll in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden."* Diese aus der Betriebswirtschaft stammende Formel zur Risikobestimmung wird auch in der Methodik der IT-Sicherheit verwendet, jedoch überwiegend nicht im Sinne einer mathematischen Formel, sondern im Sinne einer Heuristik, die am Ende dazu führt für ein Verfahren eine der drei Schutzbedarfsstufen normal, hoch oder sehr hoch festzulegen.

Die spezifischen Datenschutzrisiken bestehen darin, dass Organisationen – im vorliegenden Modellfall die Versicherung „Insight AG", die Grundrechte natürlicher Personen nicht wirksam beachten. Beurteilbar wird eine unwirksame Umsetzung von Grundrechten, wenn gegen Datenschutzrecht verstoßen wird. Das Datenschutzrecht listet, bspw. in Artikel 5 DSGVO, Grundsätze des Datenschutzes auf.

Datenschutz-Grundverordnung (vom 27. April 2016)

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Die Negation dieser verschiedenen abstrakten Grundsätze überführt diese in verschiedene konkrete, operationalisierte Risiko-Kriterien: So führt bspw. Intransparenz (Abs. 1a) eines Verfahrens – also die Intransparenz der im Verfahren verwendeten Datenbestände, IT-Systeme und Prozesse –, zur mangelhaften Kontrollierbarkeit, Prüfbarkeit und letztlich Beurteilbarkeit eines Verfahrens. Eine mangelhafte Zweckbindung (Abs. 1b) eines Verfahrens führt, wie auch mangelhafte Vertraulichkeit (Abs. 1f) durch unbefugten Zugriff, zu einem Kontrollverlust für natürliche Personen im Allgemeinen bzw. für die betroffene Kfz-Halter im Konkreten. Besteht die Möglichkeit solcher Zugriffe, kann eine betroffene Person nicht mehr abschätzen, wer was über sie weiß. Dies wäre unvereinbar mit dem Grundgesetz bzw. der EU-Grundrechte-Charta (2010). Mangelhafte Integrität (Abs. 1d, 1f) eines Verfahrens liegt dann vor, wenn eine Organisation das Verfahren operativ nicht beherrscht. Eine mangelhafte Beherrschung ist dann gegeben, wenn nicht hinreichende Schutzmaßnahmen bestehen, die sicherstellen, dass bspw. die Daten der Kunden korrekt sind; dass die IT-Systeme korrekt rechnen und auch genau nur das ausführen, was die Spezifikation, die in dem Modellfall die „Insight AG“ zu verantworten hat, vorgibt, dass die Prozesse des laufenden Betriebs korrekt ausgeführt werden und bei Fehlern, gleich welcher Art und welchen Umfangs, die richtigen Korrekturen durchgeführt werden. Das alles setzt bspw. das Vorhandensein eines IT-Sicherheitsmanagement(systems) und eines Datenschutzmanagement(systems), die mit einem hinreichenden Reifegrad installiert und betrieben wer-

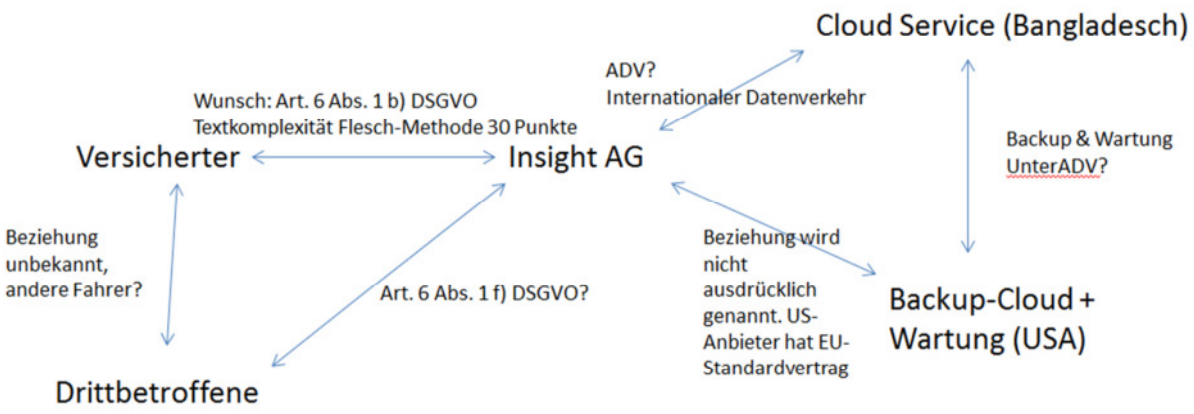
den, voraus. Ein weiteres Risiko besteht darin, wenn Daten in personenbezogenen Verfahren nicht berichtigt oder gelöscht (Abs. 1d) werden (können), bspw. auch, nachdem die Integrität eines Verfahrens durch unberechtigten oder unbefugten Zugriff angetastet wurde.

Neben Artikel 5 listet die DSGVO weitere Aspekte in Bezug auf technisch-organisatorische Anforderungen aus, die vom Standard-Datenschutzmodell auf der einen Seite zu Gewährleistungszielen generalisiert sind und die auf der anderen Seite durch Schutzmaßnahmen zur Bearbeitung dieser Ziele konkretisiert sind.[9] Aus diesen konkret-operativen Risiken, die Organisationen bei personenbezogenen Verfahren unabwendbar für Betroffene erzeugen, können dann die eingangs aufgelisteten unmittelbaren Schäden für Betroffene entstehen.

1.5 Rechtsgrundlagen

Lösungsskizze

Abbildung 4 Skizze des Sachverhalts (Rechtsbeziehungen)



1.5.1. Prüfung der Verarbeitung zum Zwecke der Berechnung eines Scores

A. Anwendbarkeit der DSGVO

I. Sachlich, Art. 2 DSGVO

1. Personenbezogene Daten

Es werden personenbezogene Daten verarbeitet. Dies ist sogar nach der gemeinsamen Erklärung von Aufsichtsbehörden und VDA der Fall, weil die Fahrzeugidentifikationsnummer unter den verarbeiteten Daten ist.[10] Diese oder ein anderer Identifika-

[9] Siehe zur Verankerung der Gewährleistungsziele in der DSGVO Kap. 6.4, S. 27 im SDM-Methodikhandbuch, V1.0

[10] Vgl. https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html

tor ist auch notwendig, da der Score zur Berechnung eines Rabattes für den Versicherungsnehmer genutzt werden soll.

2. Persönliche und familiäre Tätigkeiten

Es liegt keine persönliche oder familiäre Tätigkeit der Versicherung vor.

II. Örtlich, Art. 3 DSGVO

Es ist davon auszugehen, dass die DSGVO auch räumlich anwendbar ist.

B. Rechtmäßigkeit der Datenverarbeitung

Die Datenverarbeitung kann nach Art. 6 Abs. 1 S. 1 DSGVO nur dann rechtmäßig sein, wenn eine Rechtsgrundlage oder Einwilligung vorliegt (sog. Verbot mit Erlaubnisvorbehalt).

I. Rechtsgrundlage oder Einwilligung

1. Gewünscht: Erforderlichkeit zur Erfüllung eines Vertrages, (Art. 6 Abs. 1 b DSGVO)

a. Vertrag

Ein Vertrag zwischen Versicherungsnehmer und Versicherung kann unproblematisch geschlossen werden.

Ein Vertrag könnte nicht die Einbeziehung vermuteter Ethnie und vermutetem Geschlechts in die Berechnung des Scores rechtfertigen. Der Vertrag würde insoweit gegen § 19 Abs. 1 Nr. 2 AGG verstoßen. Ansonsten ist kein gesetzliches Verbot im Sinne von § 134 BGB ersichtlich.

Darüber hinaus liegt kein Vertragsentwurf vor. Der genaue Vertragsinhalt ist deshalb unbekannt. Die einzige Information zum Vertrag besteht in der Angabe der Textkomplexität, die nach der Flesch-Methode bei 30 Punkten liegt. Der Flesch-Wert ergibt sich aus der durchschnittlichen Silbenlänge pro Wort und der durchschnittlichen Satzlänge, die in eine auf die jeweilige Sprache abgestimmte Formel eingetragen werden. Je höher das Ergebnis ist, desto leichter ist der Text verständlich. Ein Wert von 0-30 entspricht einer sehr schweren Lesbarkeit, ein Wert von 30-50 einer schweren Lesbarkeit. Der Wert von 30 liegt damit auf der Schwelle von der sehr schweren zur schweren Lesbarkeit.[11]

Es ist unklar, inwiefern diese Information hier hilfreich sein soll. Sie könnte relevant sein, wenn eine informierte Einwilligung zu prüfen wäre, da im Rahmen der Informiertheit zu prüfen wäre, ob die der betroffenen Person zur Verfügung gestellten Informationen verständlich wären. Auch dann wäre allerdings fraglich, ob Durchschnittswerte über Silbenanzahl pro Wort und Satzlänge die relevanten Maßstäbe sind. Auch ein sehr einfacher Text enthält ggf. nicht die relevanten Informationen. Hier soll die Datenverarbeitung allerdings auf einen Vertrag gestützt werden. Art. 6 Abs. 1 b) DSGVO stellt an den Vertrag keine besonderen Anforderungen hinsichtlich

[11] https://de.wikipedia.org/wiki/Lesbarkeitsindex#Flesch-Reading-Ease

einer einfachen Sprache. Solche Anforderungen könnten sich aber aus dem Transparenzgebot des Art. 5 Abs. 1 a) DSGVO ergeben. Die Frage kann hier dahinstehen, da keine Details aus dem Vertrag bekannt sind.

b. Erforderlichkeit

Auch die Prüfung der Erforderlichkeit kann mangels Vertragstexts nur angerissen werden. In der Literatur werden für die Prüfung der Erforderlichkeit unterschiedlich strenge Maßstäbe herangezogen. Richtigerweise ist im Sinne einer Datenminimierung darzulegen, inwiefern die Erfüllung des Vertrages ohne das jeweilige Datum unzumutbar ist. Eine Prüfung der Erforderlichkeit kann hier allerdings nicht erfolgen.

Der Sachverhalt enthält nämlich keine Angaben dazu, inwiefern die aus dem CAN-Bus ausgelesenen Daten zur Berechnung des Scorewertes erforderlich sind. Hier ist von den entsprechenden Abteilungen der Insight AG der Projektgruppe darzulegen, inwieweit die einzelnen Daten jeweils erforderlich sind.

Darüber hinaus hat der Verantwortliche darzulegen, inwiefern die Aufbewahrung der Daten für 3 Jahre erforderlich ist. Es steht allerdings zu vermuten, dass dies auf der regelmäßigen Verjährungsfrist des § 195 BGB beruht.

c. Drittbetroffene

Fahrzeuge werden sehr selten ausschließlich durch den Vertragspartner der jeweiligen Kfz-Versicherung genutzt. Die Insight AG muss daher berücksichtigen, dass auch Familienmitglieder, Freunde und sonstige Dritte das versicherte Fahrzeug fahren und somit auch personenbezogene Daten über diese Personen erhoben werden. Anhand der erhobenen Daten dürfte ein Driver Fingerprinting[12] ohne weiteres möglich sein. Unabhängig davon, ob die Versicherung ein solches Fingerprinting durchführt, reicht die Möglichkeit aus, um die Daten auch in Hinblick auf Drittbetroffene als personenbeziehbar einzustufen. Ein Vertrag zwischen der Insight AG und dem Versicherten vermag diese Datenverarbeitung nicht zu rechtfertigen. Dies ergibt sich aus dem Wortlaut von Art. 6 Abs. 1 b), wonach die betroffene Person Vertragspartei sein muss.

2. Interessenabwägung für Drittbetroffene

Neben der Einwilligung, die nicht praktikabel ist, weil der Kreis der Drittbetroffenen nicht im Vorwege in jedem Fall bestimmt werden kann, kommt nur noch Art. 6 Abs. 1 f) DSGVO als mögliche Rechtsgrundlage in Betracht. Danach ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und eine Abwägung ergibt, dass die Interessen und Grundrechte und Grundfreiheiten der betroffenen Personen nicht überwiegen.

[12] http://www.autosec.org/pubs/fingerprint.pdf

Das Interesse, einen Pay-as-you-drive-Tarif anzubieten, ist zumindest von der Berufsfreiheit und der unternehmerischen Freiheit nach Art. 12 GG und Art. 16 Grundrechte-Charta (GrCH) geschützt und daher ein berechtigtes Interesse.

Auf Seiten der betroffenen Personen ist zumindest das Grundrecht auf Datenschutz nach Art. 8 GrCH betroffen.

Die Abwägung ist durch die Insight AG vorzunehmen und von Aufsichtsbehörden und Gerichten überprüfbar. Es ist von ihr darzulegen, dass die Betroffeneninteressen nicht ihre berechtigten Interessen überwiegen. Dabei wird insbesondere die hohe Individualisierbarkeit der Daten und somit ein möglicherweise fahrzeugübergreifendes Tracking zu berücksichtigen sein. Auch hier kann noch keine abschließende Beurteilung erfolgen. Es sei aber bereits angedeutet, dass die konkrete Ausgestaltung des Verfahrens hier entscheidend sein dürfte- mehr dazu beim Schutzbedarf und den Maßnahmen.

II. Automatisierte Entscheidung im Einzelfall

Es liegt durch das Scoring eine automatisierte Entscheidung im Einzelfall vor, die durch die damit möglicherweise verbundene Nichtgewährung von Rabatten den Betroffenen auch erheblich beeinträchtigen kann, Art. 22 Abs. 1 DSGVO. Dies ist auch dann der Fall, wenn man Art. 22 Abs. 1 DSGVO mit Erwägungsgrund 71 dahingehend einschränkend auslegt, dass die Einzelentscheidung unter Bewertung von Persönlichkeitsaspekten vorgenommen werden muss. Bei dem Fahrverhalten handelt es sich um einen solchen Aspekt der Persönlichkeit.

Art. 22 Abs. 1 DSGVO betrifft aber nur die Nutzung der Daten, weshalb hier zunächst Art. 6 DSGVO zu prüfen war.

Diese ist grundsätzlich verboten, allerdings könnte hier, je nach konkreter Vertragsgestaltung, die Ausnahme des Art. 22 Abs. 2 a) DSGVO greifen. Hinsichtlich der Drittbetroffenen könnte argumentiert werden, dass keine einer rechtlichen Wirkung ähnliche Beeinträchtigung vorliegt, da diesen kein Rabatt ausgeschlagen werden kann.

III. Einbeziehung weiterer Dienstleister

Die Insight AG bedient sich zur Verarbeitung der Daten eines Dienstleisters in Bangladesch, für den wiederum ein Backup- und Wartungsservice in den USA besteht. Bei dieser Konstellation sind Auftragsverarbeitungsverträge gem. Art. 28 Abs. 3 DSGVO zu schließen. Der Backup- und Wartungsservice scheint bislang als Unterauftrag ausgestaltet zu sein, weshalb ein entsprechender Unterauftragsvertrag abzuschließen ist. Die Insight AG hat hierzu ihre schriftliche Genehmigung zu erteilen, Art. 28 Abs. 2 S.1 DSGVO. Dabei sollten die zu treffenden technischen und organisatorischen Maßnahmen in den Vertrag aufgenommen werden.[13]

Eine gemeinsame Mittel- und Zweckfestlegung nach Art. 26 DSGVO ist bislang nicht ersichtlich, sollte aber im Verlauf der weiteren Konkretisierung des Sachverhalts während des Projektverlaufs fortlaufend geprüft werden.

[13] Vgl. Hartung, in: Kühling/Buchner, DSGVO, 1. Aufl. 2017, Art. 28 Rn. 71.

IV. Internationaler Datenverkehr

Über die Einhaltung der sonstigen Vorschriften der DSGVO hinaus sind bei Übermittlungen personenbezogener Daten in Drittländer die Art. 44 ff. DSGVO einzuhalten (Zweistufenprüfung). Die Vorschriften über technische und organisatorische Maßnahmen solcher Übermittlungen, nämlich nach Bangladesch und in die USA, sollen Anwendung finden. Das Ziel der Vorschriften über die Datenübermittlung an Drittländer oder internationale Organisationen ist, dass das durch die Verordnung gewährleistete Schutzniveau nicht untergraben wird, Art. 44 S. 2 DSGVO.

1. Bangladesch

Nachfolgend wird von einer Datenübermittlung nach Bangladesch ausgegangen. Ausweislich des Sachverhalts liegt dort der Firmensitz des Cloud-Betreibers. Mangels entgegenstehender Angaben wird deshalb davon ausgegangen, dass die Datenverarbeitung dort stattfinden soll.

Die Übermittlung der Daten nach Bangladesch muss daher die Voraussetzungen der Art. 44 ff. DSGVO erfüllen.

Ein Angemessenheitsbeschluss nach Art. 45 DSGVO liegt nicht vor.

Im Sachverhalt sind keine Angaben enthalten, aus denen sich ein Vorliegen geeigneter Garantien nach Art. 46 DSGVO ergibt. Diese sollten geschaffen werden.

Soweit keine Garantien geschaffen werden, könnte die Übermittlung auf Art. 49 Abs. 1 b) gestützt werden. Dazu müsste die Übermittlung an den Dienstleister in Bangladesch Vertragsinhalt werden, was ggf. eine überraschende AGB-Klausel darstellen kann. Darüber hinaus kann auch diese Norm die Übermittlung nur im Verhältnis zwischen Insight AG und Versicherungsnehmer rechtfertigen. Da hier noch Drittbetroffene existieren, kann die Übermittlung nicht auf Art. 49 Abs. 1 b) gestützt werden.

2. USA

Bei der Übermittlung in die USA ist der Sachverhalt etwas unklar. Hier wird davon ausgegangen, dass es sich um einen Unterauftragnehmer des Dienstleisters in Bangladesch handelt.

Für die USA liegt mit dem Privacy Shield ein Angemessenheitsbeschluss der Kommission vor. Es ist allerdings absehbar, dass dieser vor dem Hintergrund der im Schrems-Urteil formulierten Anforderungen an solche Beschlüsse mittelfristig wieder durch den EuGH überprüft werden wird.

Allerdings besitzt der Dienstleister in den USA ausweislich des Sachverhalts einen EU-Standardvertrag. Entgegen dem Wortlaut von Art. 46 Abs. 1 DSGVO dürfte die Norm nicht nur dann anwendbar sein, wenn kein Angemessenheitsbeschluss vorliegt. Im Gegenteil dürfte es zu begrüßen sein, wenn der Verantwortliche Unsicherheiten bezüglich der Wirksamkeit eines Angemessenheitsbeschlusses durch Schaffung von Garantien nach Art. 46 DSGVO ausgleichen möchte. Eine solche Garantie kann hier durch Abschluss eines Standardvertrags nach Art. 46 Abs. 2 c) DSGVO geschaffen werden.

V. Ergebnis

Aus dem vorliegenden Sachverhalt ergeben sich, wie aufgezeigt, erhebliche rechtliche Risiken. Im weiteren Verlauf der DSFA werden Möglichkeiten aufgezeigt, mit diesen Risiken umzugehen.

1.5.2. Prüfung der Verarbeitung zum Zwecke der Unfallforschung und Weiterentwicklung der Algorithmen

A. Anwendbarkeit der DSGVO

Ausweislich des Sachverhalts soll eine Anonymisierung durch Entfernung der Fahrgestellnummer vorgenommen werden. Dies ist vor dem Hintergrund der umfangreichen Profilbildung nicht ausreichend. Dem steht auch nicht die gemeinsame Erklärung von Aufsichtsbehörden und VDA entgegen, da dort lediglich vereinbart wurde, dass ein Personenbezug zumindest dann besteht, wenn Daten mit der Fahrzeugidentifikationsnummer verknüpft sind. Es besteht hier die hohe Wahrscheinlichkeit, dass sich aus den erhobenen Daten hochindividualisierte Fahrprofile ergeben, die dann wieder Individuen zugeordnet werden können. Dies kann z.B. dann der Fall sein, wenn ein Drittbetroffener ebenfalls Kunde der Insight AG ist und den Telematiktarif gebucht hat.

Daher ist zu prüfen, ob eine wirkliche Anonymisierung hier möglich ist. Zur Unfallforschung dürften aggregierte Daten ohne Personenbezug beispielsweise ausreichen. Sollte dies nicht der Fall sein, wären die Daten zu löschen oder die weitere Verarbeitung durch eine Rechtsgrundlage zu rechtfertigen.

Mangels Grundlage im Sachverhalt kann hier keine weitere Prüfung erfolgen.

B. Zwischenergebnis

Es liegen personenbezogene Daten vor. Sollen die Daten dennoch in dieser Form für Zwecke der Unfallforschung und Algorithmenverbesserung verarbeitet werden, wäre das Datenschutzrecht anwendbar.

2. Bewertung

In dieser Phase werden die Kriterien für die Bewertung der Risiken des Verfahrens ausgewiesen und dann beurteilt.

Da mit dem Verfahren bereits eine eingriffsintensive Verarbeitung personenbezogener Daten durch die Versicherung, und die anderen beteiligten Organisationen, vorliegt und somit das Risiko der Beeinträchtigung der Risiken und Freiheiten betroffener Personen durch die Organisation bereits festgestellt ist**, ist die funktionale Ausgestaltung des Verfahrens und die Umsetzung der Schutzmaßnahmen, für jedes der Gewährleistungsziele und dem Schutzbedarf entsprechend, durch jede der beteiligten Organisationen von vornherein obligatorisch.** Darüber hinaus bedarf es einer weiteren Auflistung und Bewertung von zusätzlichen Risiken, die insbesondere aus der Nutzung einer (unsicheren) IT bei den verschiedenen Organisationen entstehen, um die Art und Detailtiefe von Schutzmaßnahmen auch der IT-Sicherheit, die sowohl im Interesse der Organisation als auch der Betroffenen liegt, zu bestimmen (siehe die Begründung der Bewertungsrisiken auf S. 15).

Die Auflistung und Beurteilung von Risiken konzentriert sich nachfolgend auf Aspekte der Risiken für Betroffene, die insbesondere aus der Nichtverfügbarkeit des Verfahrens, aus Fehlern und unbefugter Kenntnisnahme bei der Erhebung, Berechnung und Übermittlung von Daten, aus Intransparenz der Datenverarbeitung, aus der Nichtumsetzung von Betroffenenrechten und der Zwecküberdehnung der Datennutzung entstehen können.

2.1. Identifikation der Bewertungsmaßstäbe anhand der Schutzziele

Das Verfahren wird anhand der Gewährleistungsziele des SDM durchgeführt und auf den Modellfall hin spezifiziert.

Verlangt wird die Sicherung des Verfahrens in Bezug zur:

- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Transparenz
- Nichtverkettung
- Intervenierbarkeit

Dass diese Gewährleistungsziele als verdichtete normative und operativ zugängliche Anforderungen nutzbar sind, ist mit Hilfe der Mapping-Tabelle im SDM-Handbuch – mit Verweisen auf die jeweiligen Artikel der DSGVO – belegt (vgl. SDM-Handbuch V1.0, S. 29).

Weitere konkrete Anforderungen in Bezug auf die Durchsetzung eines operativen Datenschutzes, als die von den Gewährleistungszielen bereits erfassten, sind nicht ersichtlich, ein Verzicht auf die Beachtung eines oder mehrerer dieser Gewährleistungsziele ist nicht zu rechtfertigen.

Nach SDM ist zu beachten, dass die Bewertungsmaßstäbe sich nicht nur auf den Datenbestand beschränken, sondern das Verfahren insgesamt, und somit neben den Daten auch IT-Systeme und Prozesse betreffen.

2.2. Identifikation möglicher Missbrauchsszenarien

Das DSFA-Framework spricht in Bezug auf Organisationen und deren Verantwortliche von „Angreifern“. Der Begriff des „Angreifers“ entstammt dem akademischen Diskurs über Risiken der Informationssicherheit und ist dort die gängige Bezeichnung für jeden Akteur, der – absichtlich oder unabsichtlich – die jeweiligen Schutzziele verletzt. Der Begriff beschränkt sich mit Bezug auf Datenschutz nicht nur auf unautorisierte externe Angreifer, die ein System vorsätzlich und häufig mit kriminellen Absichten angreifen („Cracker“), sondern bezieht sich auch auf Organisationen, die vorsätzlich oder fahrlässig insbesondere intransparent, ohne den Betroffenen wirksame Einflussmöglichkeiten einzurichten und zwecküberdehnend agieren können sowie vielfach auch immer noch nicht hinreichende Maßnahmen der IT-Sicherheit umgesetzt haben.

Die nachfolgende Benennung möglicher Missbrauchsszenarien dient nicht dazu, den beteiligten Stellen ein rechtswidriges Verhalten zu unterstellen. Das ist in diesem Stadium auch noch gar nicht möglich. Allerdings kann der Verantwortliche nur dann angemessene Schutzmaßnahmen treffen, wenn er alle sinnvoll in Betracht kommenden Missbrauchsszenarien bedenkt. In diesem Rahmen ist selbstverständlich auch rechtswidriges Verhalten zu berücksichtigen.

Personenbezogene Bewegungsprofile sind generell für Organisationen von Interesse, etwa um Werbung einzuspielen oder das Profil von Person auch für ein Risikomanagement in anderen Lebensbereichen nutzen zu können. Grundsätzliches Interesse dürften Plattformbetreiber an diesen Real-world-Daten haben, deren Geschäftsmodell – zwecks Verschneidens mit den Online-Daten – in der Verarbeitung personenbezogener Daten besteht.[14]

a) Versicherung

Das Hauptmotiv der Versicherung besteht darin die Risiken, die durch den Kfz-Halter, der die Versicherungspolice bezahlt, erzeugt werden, in Gewinnerzielungsabsicht so genau wie möglich bestimmen zu können. Im Modellkontext heißt das: Je genauer die Bewegung des Kfz durch fahrerspezifische und kontextuale Eigenschaften kontrolliert werden (#RV01)[15], desto differenzierter kann der Versicherungsbeitrag gestaltet werden. Dabei besteht grundsätzlich, wie bei allen Unternehmen, ein strukturelles Interesse zum einen an einer Zweckdehnung oder Änderung von Zwecken und damit an einer Erweiterung des Datenumfangs über das erforderliche Maß hinaus (#RV02), an der Intransparenz des Verfahrens (#RV03), ausgewiesen als Betriebsgeheimnis gegenüber Konkurrenten, sowie Interesse an der Robustheit des Verfahrens gegenüber den Rechten, Interessen und Bedürfnissen betroffener Personen (#RV04), zum Zweck der Kosteneinsparungen durch ein weitgehend automatisiertes Verfahren. Diese Risiken würde man als Betroffener bei der Versicherung als Verantwortlichem adressieren. Dass diese Risiken der Intransparenz aus dem Binnenverhältnis etwa zwischen der Versicherung und dem Scorebox-Hersteller herrühren können, muss die Versicherung im Binnenverhältnis zu ihrem Auftragnehmer bearbeiten.

[14] Solche Plattformbetreiber ließen sich in einem erweiterten Angreifermodell thematisieren, in dem auch solche Angreifer zu betrachten wären, die in keinem ersichtlich unmittelbaren Bezug zum Verfahren stehen, aber die den Anreiz für die internen Angreifer setzen.

[15] Bei den nachfolgend in Klammern gesetzten #Bezeichnern (wie bspw. „#RV01“) handelt es sich um Kürzel, die die identifizierten Risiken adressieren. Im Kapitel 4.1 zur Erstellung eines DSFA-Berichts sind alle derartig adressierten Risiken, nach Beteiligten und Gewährleistungszielen, aufgelistet.

Zu beachten ist zudem der Aspekt der Weitergabe von (Teilmengen der) personenbezogenen Daten, etwa an andere Teile einer Versicherungsholding, an Banken bzgl. Kreditsicherung oder an Kfz-Leasingunternehmen.[16] (#RV05)

Wenn Mitarbeiter ihre Kfz beim eigenen Arbeitgeber versichern, können möglicherweise Dienstvorgesetzte Einsicht in das private Fahrverhalten von Mitarbeitern nehmen (Mitarbeiterdatenschutz). (#RV06)

Durch Geolokalisation des Kfz können weitere externe Versicherungsrisiken hinzukommen, wie bspw. häufige oder lange Auslandsaufenthalte des Kfz mit zusätzlichen Risiken (Diebstahl), die weitetere Datenschutzrisiken auch für die Betroffenen bedeuten. Die Geolokalisation darf im Regelfall allein die Versicherung vornehmen, sie kann jedoch auf unterschiedlichen Ebenen von allen beteiligten Organisationen vorgenommen werden, sofern keine Schutzmaßnahmen getroffen wurden. (#RV07)

Es sind Konstellationen denkbar, wonach Mitarbeiter (Sachbearbeitung, Leitung, Administration) Interesse an der Übermittlung von Daten (Vertraulichkeitsbruch), an deren Änderung (Integritätsverlust) sowie deren Nutzung in anderen Kontexten der Versicherung haben können, weil sie in einem besonders engen Kontakt oder im Gegenteil in einem dezidiert missgünstigen Verhältnis zum Versicherungsnehmer stehen. (#RV08)

b) Kfz-Inhaber, Fahrzeugführer und Mitfahrer

Ein Zweitfahrer hätte bei Zugriff auf die erhobenen Daten (z.B. per App über die OBD2-Schnittstelle) eine Möglichkeit, das Fahrverhalten der anderen Fahrer bzw. deren Nutzungsgewohnheiten einzusehen, z.B. über die gefahrenen Strecken zur Kontrolle einer Fahrstrecke aus Eifersucht. (#RM01)

Im Sachverhalt ist von einer App die Rede, über die jedoch keine weiteren Informationen zur Funktionalität vorliegen. Es ist also bislang unklar, wer unter welchen Voraussetzungen ggf. Zugriff auf die über die App abrufbaren Daten hat.

Mitfahrer sollten in Kenntnis gesetzt werden, dass sämtliche Kfz-Eigenschaften bzgl. einer Fahrt gespeichert und ausgewertet werden und vermutlich auch Beifahrern, etwa durch Erheben der Belastung der Sitze (Körpergewicht), zugeordnet werden können. (#RM02)

Da sich der Score auf Grundlage automatisierter Einzelentscheidungen berechnet, im Verfahren selbst aber keine explizite Unterscheidung verschiedener Fahrer vorgenommen, sondern nur „vermutet“ wird, kann ein Zweitfahrer den Score beeinflussen und beispielsweise (un)beabsichtigt verhindern, dass die Prämie am Jahresende gewährt wird. Die Unterscheidung zweier Fahrer, die dasselbe Kfz nutzen, kann zudem durch das Verfahren lediglich im Nachhinein erfolgen und das auch nur für den Fall, dass genügend Daten für eine Differenzierung gesammelt wurden. (#RM03)

Inwiefern es hier Widerspruchsmöglichkeiten oder Möglichkeiten einer Stellungnahme gibt, lässt sich aus dem geschilderten Sachverhalt nicht erschließen.

c) Kfz-Kontext (Vertragswerkstätten und „Schrauber“)

[16] Hinweis: Facebook bietet die Nutzung einer Rangliste zu Fahrverhalten anhand von Daten, die Facebook-nutzende Fahrer selbst erheben und die sich mit Versicherungsdaten verschneiden lassen.

Werkstätten können zum Auslesen des Kfz-Zustands auf die OBD2-Schnittstelle zugreifen und somit grundsätzlich auch auf die Daten zur Errechnung des Fahrverhaltenscores zugreifen sowie eine Geolokalisation durchführen. Zugleich können Werkstätten veranlasst werden, die OBD2-Schnittstelle und die Scorebox auf Standard-Funktionalitäten und ein Standard-Set an abrufbaren Daten zu prüfen und die zu quittieren. (#RW01)

Es ist unklar, welche Daten in der Scorebox eines Kfz seitens der Kfz-Hersteller noch erzeugt und gespeichert und über die OBD2-Schnittstelle ausgelesen werden können. Die Insight AG ist gehalten darauf hinzuwirken, dass die von ihnen beauftragten Kfz-Werkstätten nur die erforderlichen Daten auslesen und den Umfang der ausgelesen Daten bspw. quittieren können. (#RW02)

Auch das Tunen von Kfz, insbesondere durch darauf spezialisierte Kfz-Werkstätten, wäre zu berücksichtigen. Hier könnte Leistung gesteigert werden, ohne dass die Sensorik entsprechend korrekte Daten erzeugt. (#RW03)

Zu prüfen wäre außerdem, inwieweit Werkstätten auch schreibend auf die OBD2-Schnittstelle zugreifen können, soweit es um die Kfz-Daten geht. (#RW04)

Es sind Motive denkbar, wonach Mitarbeiter von Kfz-Werkstätten Interesse an der Übermittlung von Daten (Vertraulichkeitsbruch bspw. durch den Verkauf von Daten, gezielte Überwachung von Fahrern), an deren Änderung (Integritätsverlust bspw. in Bezug auf das Verbergen von Motortuning oder das Auslesen korrekter Sensordaten) sowie Nutzung in anderen Kontexten (Verkettung) haben können. Hierbei wäre der Zugriff auf die OBD2-Schnittstelle vom Zugriff auf die Scorebox zu unterscheiden (#RW05).

d) Hersteller der Scorebox (inkl. Funkkomponente)

Der Scorebox-Hersteller hat den operativ größten Einfluss auf die Verarbeitung der Kfz-Daten an der OBD2-Schnittstelle und kann darüber hinaus boxeigene Daten durch boxeigene Sensoren (bspw. GPS-Daten, sollten diese seitens der OBD2-Schnittstelle nicht bereits angeliefert werden oder Beschleunigungssensoren, Batteriespannungssensoren, Wettersensoren) erzeugen und auch zusätzliche Kontextinformationen erheben (bspw. durch den personenbeziehbaren Download von Straßenkartenmaterial aus dem Internet). Beim Scorebox-Hersteller sind alle operativen Risiken der IT-Sicherheit und des Datenschutzes zu ermitteln und zu bearbeiten. (#RHS01)

Die Kopplung der eindeutig dem Kfz-Halter zugeordneten Scorebox (Scorebox-Identnummer), der Vergabequelle (Hersteller, Versicherung, Kfz-Werkstatt) und der Kfz-Fahrzeugnummer muss datenschutzgerecht realisiert werden. (#RHS02)

Ein grundsätzlich bestehendes Motiv für den Funk-Tool-Hersteller ist die Geolokalisation des Halters. Ein Motiv könnte das Anbieten von *location based services* im hochauflösenden Sekundentakt sein, ebenso das Anbieten spezieller Verfolgungsservices für Sicherheitsbehörden. (#RF01)

Zusätzliche Tools auf der Funkkomponente könnten weitere Daten erzeugen und diese mit den Kfz-Daten anreichern.

e) Provider bzgl. der Datenfunkübertragung

Ein grundsätzlich bestehendes Motiv für Kommunikationsprovider ist ebenfalls die Geolokalisation des Halters. Ein Motiv könnte auch hier das Anbieten von *location based services* im hochauflösenden Sekundentakt sein, ebenso das Anbieten spezieller Verfolgungsservices für Sicherheitsbehörden. (#RP01)

Ein weiteres Risiko ist die unbefugte Kenntnisnahme (#RP02) und eine Verletzung der Integrität (#RP03) der Kfz-Daten sowie die Verknüpfung mit dem Kfz-Halter (#RP04).

f) Cloud-Betreiber

Ein Cloud-Betreiber ist grundsätzlich in der Lage auf Daten, die in seinem operativen Hoheitsbereich gespeichert und berechnet werden, zuzugreifen (#RC01). Wenn neben den Daten aus dem Kfz auch die Kfz-Handynummer, zwecks Zuordnung von Datensätzen, übermittelt würde, liegt trotz einer eventuell zum Einsatz kommenden Verschlüsselung bereits innerhalb der Scorebox ein unmittelbarer Personenbezug vor. Es liegen in jedem Falle personenbeziehbare Daten vor, da über den Schlüssel der Personenbezug hergestellt werden könnte. Der Cloud-Betreiber kann anhand der eintreffenden Datenpakete von Fahrten eine eigene Form des Profiling des Fahrverhaltens des Kfz-Halters erstellen (Zeitpunkte, Dauer, Routinen).

Wenn der Cloud-Betreiber auch für andere Organisationen, die andere Dienstleistungsinhalte für einen Versicherungsteilnehmer erbringen, Rechenleistungen erbringt, könnte das Kfz-Profil mit anderen Profilen anderer Dienstleistungen verschnitten werden. (#RC02)

Für den zweiten Cloud-Betreiber, der die Verfügbarkeit der Kfz-Daten sichern soll, gilt das Gleiche wie für den ersten Cloud-Betreiber.

g) Sicherheitsbehörden

Sicherheitsbehörden können durch den Zugriff auf die Kfz-Daten die Aufenthaltsorte und Aufenthaltszeiten eines Kfz und damit wahrscheinlich auch eines im Verdacht stehenden Fahrers bestimmen. Ferner könnten die Behörden direkt Daten zu möglicherweise sanktionierbarem Fehlverhalten im Verkehr (z.B. Überschreitung der zulässigen Höchstgeschwindigkeit) gewinnen. Als ein weiterer Umstand wäre zu berücksichtigen, dass bei der vorgesehenen Cloud-Lösung auch nichteuropäische Sicherheitsbehörden ins Spiel kämen, die auf diese Daten nationalrechtlich gedeckt zugreifen dürfen und können. Bei einem Zugriff durch Dritte stellt sich nicht nur die Frage nach der Sicherung der Berechtigung, sondern auch die nach Sicherung der Transparenz und Integrität. (#RS01)

h) Hacking (Zugriff durch unbeteiligte Dritte, insbesondere aufgrund unsicherer IT)

Hacker können Daten an verschiedenen Stellen – direkt am Kfz/OBD2-Schnittstelle, über eine Werkstatt, die Clouds, die interne IT (Programme, Hardware, Schnittstellen) der Versicherung – auf die Kfz- oder die Fahrer-Daten zugreifen. (#RH01)

Für die Veränderung der Daten gibt es vielfältige Motive: Änderung von Daten, Prozessen, IT-Systemen zur Erzeugung der Scorewerte im Auftrag von Betroffenen oder auch zur Erpressung der Versicherung bzgl. des Vermeidens von falschen, ruinösen Berechnungen.

Die Überlegungen gehören zum Kontext eines IT-Security-Impact-Assessments. Sofern eine Organisation kein Safety- und Security-Assessment durchführt, muss dieses Assessment im Rahmen der DSFA

mit erfolgen und würde dort vornehmlich Aspekte zur Sicherung der Integrität und Vertraulichkeit betreffen. Eine Versicherung, die wie die Insight AG personenbezogene Daten mit hohem Schutzbedarf verarbeitet, muss schlicht über ein eigenständiges IT-Sicherheitsmanagement verfügen, das im Wesentlichen auf dem Schutz der Geschäftsprozesse ausgerichtet ist und somit im eigenen Interesse der Organisation liegt. Dabei ist zu beachten, dass die aus einem IT-Security-Assessment abgeleiteten Schutzmaßnahmen anschließend einer weiteren DSFA zu unterziehen, da auch die Maßnahmen der IT-Sicherheit den Anforderungen von Art. 5 und 32 DSGVO genügen müssen. Hierbei können sich insbesondere Unterschiede bei der Schutzbedarfsbestimmung ergeben, da die DSGVO hierfür auf die Risiken für die Rechte und Freiheiten der betroffenen Personen abstellt, während bei einer reinen IT-Sicherheitsbetrachtung Einbußen für die Insight AG maßgeblich wären.

2.3 Eingriffsintensität / Schutzbedarf

Die automatisiert maschinelle Erfassung menschlicher Handlungen bedeutet, wie zuvor schon festgestellt, eine hohe Eingriffsintensität beim Kfz-Halter seitens der verantwortlichen Versicherung.

Dem normativen Aspekt der „Eingriffsintensität“ eines Verfahrens für einen Kfz-Halter ist der operative Aspekt des „Schutzbedarfs“ zuzuordnen. Die hohe Eingriffsintensität des Verfahrens entspricht insofern dem hohen Schutzbedarf auf Seiten betroffener Personen. Der Schutzbedarf ist in diesem Fall bereits rechtlich festgelegt, diese DSFA muss bzw. soll durchgeführt werden. Insofern bedarf es für den Modellfall keiner weiteren Erwägungen zur Klärung des Schutzbedarfs.[17] Außerdem sind Aspekte der Informationssicherheit zu berücksichtigen, damit das Verfahren so sicher gestaltet wird, dass unbefugte Dritte („Cracker“) sich nicht Zugriff auf Daten bzw. das Verfahren verschaffen können.

Die Festlegung auf hohen Schutzbedarf hat Folgen für die Ausgestaltung der funktionalen Aspekte des Verfahrens und der Schutzmaßnahmen, die aufgrund der Datenschutzgrundsätze aus Art. 5 DSGVO und insbesondere der Artikel 24, 25 und 32 DSGVO mit Bezug zu TO-Maßnahmen sowie der Betroffenenrechte der Artikel 12 bis 22 umzusetzen sind. Die Nutzung von Scoring macht das Verfahren zu einem besonders schutzwürdigen Verfahren. Deshalb ist von einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen auszugehen ist (vgl. Art. 35 Abs. 3 lit. a DSGVO).

Selbst wenn die Festlegung „hoher Schutzbedarf“ nicht schon normativ erfolgte, würde der Umstand, dass im Modellfall viele Daten über massenhaft viele Betroffene unter Beteiligung vieler Stellen gesammelt an einer zentral verarbeitenden Stelle zusammengeführt werden dazu führen, dass aufgrund des Kumulationseffekts ein hoher Schutzbedarf festzusetzen ist (SDM-Handbuch, Kap. 9.5).

2.4 Bewerten des Risikos

In Bezug auf den vorliegenden Fall handelt es sich um keine Wahrscheinlichkeit des Eintritts des Risikos der Verhaltenskontrolle (bzw. spezifischer: Bewegungskontrolle), sondern bereits um einen tatsächlich erfolgenden Eingriff. Die „Schwere“ des Eingriffs (Eingriffsintensität) ist „hoch“, weil eine

[17] Das SDM unterscheidet drei Schutzbedarfsstufen: „normal“, „hoch“ und „sehr hoch“. Bei Personenbezug eins Verfahrens sind, allein weil personenbezogene Daten verarbeitet werden, bereits sämtliche Schutzmaßnahmen sämtlicher Gewährleistungsziele der Schutzbedarfsstufe „normal“ zu treffen, die bei besonders schutzwürdigen Daten oder Verfahren mit Schutzbedarf „hoch“ in ihrer Wirkung und der Kontrolle noch zu intensivieren sind. Der Schutzbedarf „sehr hoch“ ist solchen Verfahren vorbehalten, die direkten Einfluss auf Leib und Leben von Betroffenen nehmen können.

Vollkontrolle vieler Verhaltensparameter sowie der Bewegungen von Personen in dem Kfz erfolgt – und genau deshalb eine DSFA für Scoring-Verfahren durchzuführen ist. Dass die betroffene Person im Modellfall dieser Kontrolle im Rahmen eines Vertrags zustimmen würde, ändert nichts an der objektiven Eingriffsintensität des Verfahrens. Wichtig ist zudem der Umstand, dass ein solcher Vertrag nur zwischen dem Halter – über dessen Verarbeitung personenbezogener Daten – und der Versicherung besteht. Diese Konstellation ist vorliegend aber nicht immer der Fall. Es werden auch Daten von sonstigen Fahrern und Mitreisenden erhoben und verarbeitet, was spätestens dann ein datenschutzrechtliches Problem darstellt, wenn dieser durch eine der beteiligten Instanzen, insbesondere durch die Versicherung, bestimmbar sind.

Die nachfolgende Risikobewertung konzentriert sich auf die Eintrittswahrscheinlichkeit der Fremdbestimmung betroffener Personen durch die beteiligten Organisationen in Bezug auf die sieben ausgewiesenen Gewährleistungsziele (Kap. 2.1), die acht Angreiferszenarien (Kap. 2.2) sowie den Schutzbedarfs der betroffenen Personen mit „hoch“ (Kap. 2.3).

Das Risiko einer Verletzung datenschutzrechtlicher Bestimmungen lässt sich aus der Missachtung der Schutzziele – welche im Standard-Datenschutzmodell (SDM) entwickelt wurden – Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Intervenierbarkeit, Transparenz und Nichtverkettung ableiten.[18] Neben der Datenminimierung, die bei der Verarbeitung personenbezogener Daten immer bedacht werden muss, nehmen die anderen 6 Ziele je nach betrachtetem Verfahren unterschiedliche Stellenwerte ein. Auf eines der Gewährleistungsziele zu verzichten ist jedoch auf Grund der engen Bindung an die normativen Vorgaben des Gesetzgebers nicht möglich. Widersprüche oder Spannungen zwischen den einzelnen Schutzzielen aufzuzeigen und getroffene technische und organisatorische Maßnahmen (TOM) auf ihre Wirksamkeit hin zu überprüfen, trägt dazu bei, eine objektive Beurteilung des Risikos des Verfahrens erstellen zu können. So gelten für die – aus der IT-Sicherheit abgeleiteten – Ziele Verfügbarkeit, Vertraulichkeit und Integrität auch weiterhin der IT-Grundschutzkatalog und internationale technische Standards (ISO). Der Fokus liegt jedoch, wie oben bereits erwähnt, nicht auf der Abwehr von Gefahren für die Organisation sondern auf dem Schutz der betroffenen Personen als Grundrechtsträger. Auf Grund der verschiedenen Professionalisierungsgrade der beteiligten Akteure muss die Bewertung der Risiken im Hinblick auf Eintrittswahrscheinlichkeit und Häufigkeit an diese angepasst werden.

Die konkret geplanten Schutzmaßnahmen zur Verminderung der Eingriffsintensität und der Risiken – im Modellfall werden die Kfz-Daten in der Scorebox verschlüsselt – werden erst im nachfolgenden Kapitel, das der Bestimmung von Schutzmaßnahmen dient, berücksichtigt. Die eventuell auch mit installierten Schutzmaßnahmen noch verbliebenen Risiken werden als Restrisiken thematisiert.

2.4.1. Datenminimierung

Insgesamt wird eine Vielzahl an Daten erhoben, deren vermutete Aussagekraft nicht überprüfbar (z.B. Anzahl der Kneipenbesuche) ist oder die nicht erhoben werden dürfen (Geschlecht, Ethnie). (#RD01)

Unter dem Aspekt des Erstellens eines risikobasierten Scores, unbeachtet der datenschutzrechtlichen Zulässigkeit, lassen sich die meisten aufgelisteten Kfz-Daten als erforderlich rechtfertigen. Bei den

[18] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder 2016: Handbuch zur SDM-Methodik, V1.0 https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf

aus den Kfz-Daten errechneten Verhaltensdaten sind zumindest die letzten zwei Daten (Kneipenbesuche, Straßenrennen) aufgrund zweifelhafter Korrelationen problematisch. Und das Geschlecht oder die ethnische Zugehörigkeit dürfen nicht zur Risiko- bzw. Tarif-Diskriminierung genutzt werden (§ 9 Abs. 1, Nr. 2, Allgemeines Gleichbehandlungsgesetz).

Datenminimierung wird laut Kommentarlage zweistellig interpretiert: Vorrangig ist die Aufforderung, dass keine personenbezogenen Daten erhoben werden sollen, was ein Aspekt des Verbots mit Erlaubnisvorbehalt ist (vgl. Art. 6 DSGVO). Wenn das Erheben und Verarbeiten personenbezogener Daten für ein Verfahren auf einer Rechtsgrundlage berechtigt geschieht, dann müssen die im Verfahren verwendeten Daten auf das unbedingt erforderliche Maß beschränkt werden. Im vorliegenden Planspiel stand ein Methodenvergleich im Vordergrund. Deshalb wurde die weitere Untersuchung nicht bereits abgebrochen, nachdem das Übermaß an Daten, die an der OBD2-Schnittstelle abgegriffen und zu einem Scorewert verrechnet werden, festgestellt wurde.

2.4.2. Verfügbarkeit

Das Verfügbarkeitsrisiko für den Betroffenen besteht darin, dass ein Scorewert, mit dessen Ermittlung sich der Kfz-Halter vertraglich einverstanden erklärt hat, nicht erzeugt wird. Das ist nicht zwingend ein spezifisches Datenschutzproblem, sondern betrifft auch andere Rechtsgebiete (allgemeines Vertragsrecht). (#RVerf01)

Die möglichen Gründe für Ausfälle des Scorewerts sind in der gesamten Prozesskette – vom Nichtvorhandensein von Sensordaten beim Kfz, insbesondere bei denjenigen Fahrzeugen, die älter als 2001 sind oder aus anderen Gründen keine Schnittstelle aufweisen, bis zum Ausfall des Score-Berechnungsprogramms bei der Versicherung – zu bestimmen.

Das Risiko des Ausfalls (von Teilen) des Verfahrens ist grundsätzlich eher als gering einzuschätzen. Der Ausfall von Komponenten, konkret etwa durch Funklöcher, fehlerhafte Scoreboxen (#RSB01) oder durch mangelnde Redundanz bei einer der beteiligten Organisationen – der Cloud-Betreiber nutzt eine weitere Cloud (#RCVerf03), wäre für den Betroffenen unkritisch, wenn der Vertrag eine Regelung vorsähe, wonach der Ausfall von (hinreichend vielen) Scorewerten den Versicherungsbeitrag zu Gunsten des Versicherten im Sinne eines geringen Risikos angesetzt würde. Andernfalls würde dem Betroffenen auf Grund der mangelnden Verfügbarkeit der Daten ein monetärer Schaden entstehen. Die Versicherung hätte daher ein großes Interesse, auf Redundanzmaßnahmen bei den anderen Organisationen der Prozesskette zu achten.

Des Weiteren hat der Betroffene ein Recht auf Datenübertragbarkeit gemäß Art. 20 Abs. 1 DSGVO. Das bedeutet, dass der Versicherungskunde bei einem Versicherungswechsel ein Recht darauf hat, die über ihn gespeicherten personenbezogenen Daten an eine andere Versicherung übertragen zu lassen. Was dies im Detail bedeutet und ob es für Kfz-Quelldaten oder auch Versicherungsscores gelten soll, wäre genauer zu betrachten, was hier nicht erfolgen soll. Aber wenn Daten zu transferieren wären, dann wären hierfür Prozesse vorzusehen, die wegen des hohen Schutzbedarfs wiederum mit dem vollständigen Katalog an Schutzmaßnahmen zur Umsetzung des operativen Datenschutzes und der IT-Sicherheit auszugestalten sind. (#RVerf03)

2.4.3. Integrität

Der Integritätsaspekt betrifft sowohl die Richtigkeit als auch die Aktualität und Authentizität der Kfz- und der Fahrer-Daten bei der Versicherung, im Kfz-Kontext, beim Funknetz-Provider, beim Hersteller der Scorebox, bei den Cloud-Betreibern und bei Auskunftsverlangen, bspw. durch Sicherheitsbehör-

den oder Unfallbeteiligte. Gleiches gilt für die Korrektheit der Übermittlung der Daten aus dem Kfz an die Cloud, zwischen den beiden Clouds, zwischen der Cloud und der Versicherung und ggfs. zwischen der Versicherung und einer Sicherheitsbehörde. (#RInt01)

In der Praxis würde vermutlich ein Scorewert auch dann errechnet werden, wenn die gelisteten Kfz-Daten nicht vollständig zur Verfügung stünden. Bei unvollständiger Erfassung der Kfz-Daten kann jedoch ein Integritäts-Problem bestehen, nämlich dass nicht sichergestellt ist, dass in den Phasen, in denen Sensordaten erzeugt und berücksichtigt werden, nicht nur einseitig „teure" Kfz-Eigenschaften erfasst wurden. Dies müsste die Versicherung belegen. Insofern müsste dem Betroffenen oder stellvertretend einer Aufsichtsinstanz – denkbar wären neben dem Datenschutz auch der Verbraucherschutz – grundsätzlich eine Möglichkeit eingeräumt werden, sämtliche Fahrten und sämtliche Kfz-Kennzahlen und die daraus errechneten Fahrer-Kennzahlen nachvollziehen zu können.

Die **Versicherung** hat ein Interesse an aktuellen, vollständigen und sachlich zutreffenden Daten.

Ein Risiko für den Betroffenen besteht darin, dass der Score aufgrund ungenügender Schutzmaßnahmen falsch gerechnet wird. (#RInt12)

Ein weiteres Risiko für den Betroffenen ergibt sich aus der Intransparenz des Berechnungsmodells. Das Verfahren soll mittels selbstlernender Algorithmen unter anderem Gegenden und Uhrzeiten mit erhöhtem Unfallrisiko berücksichtigen (Big Data). Es ist jedoch unklar inwieweit oder ob überhaupt der Kfz-Halter bzw. Fahrer darüber informiert wird, dass eine (zeitweise) Gegend, z.B. der Aufenthaltsort Schanzenviertel in Hamburg, als riskanter als ein Aufenthalt an anderen Orte eingestuft wird. Der Kfz-Halter bzw. Fahrer, der möglicherweise ganz bewusst risikoarm am Straßenverkehr teilnimmt, kann auf diese Faktoren nur Einfluss nehmen oder die Bereiche meiden, wenn ihm die Berechnungsgrundlagen bekannt sind und er auch über kurzfristige Änderung informiert wird. **Dieser Aspekt ist ein Beispiel für das ganz allgemein bestehende inhärente Modellierungsrisiko dieses Verfahren.**

Ein ganz anders gelagertes Risiko für den Betroffenen kann aus Missbräuchen aufgrund einer mangelhaften Umsetzung der IT-Sicherheit bei der von der Versicherung betriebenen IT entstehen. (#RInt02)

Ferner sind die Aspekte der Korrektheit der IT-Systeme, die bei den genannten Organisationen eingesetzt werden, wie auch die Korrektheit der Prozesse bis hinein in das Controlling bzgl. Datenschutz und IT-Sicherheit, einzeln abzuschätzen. Ein weiterer Risikoaspekt ist die Sicherung von Prozessen zur korrekten Übermittlung von Anweisungen der Versicherung an die Auftragnehmer und das nachweisbare Controlling der nachzuweisenden Ausführungen der Auftragnehmer (Scoreboxhersteller, Werkstätten, Funknetzprovider, und Cloud-Betreiber. (#RInt11) Diese ersichtlich überbordende Komplexität bei der Sicherung der integren Erhebung, Speicherung, Übermittlung und Berechnung von Daten und des dazu notwendigen Controllings der IT-Systeme und Prozesse einschließlich des Abschätzvorgangs selber führt in seiner Gänze dazu, dass ein generell hohes Risiko bzgl. der Integrität des Verfahrens für Betroffene besteht.

Auch zu beachten ist das Risiko, dass Datenschutzvorfälle nicht gemeldet werden. (#RInt13, #RTrans04, #RTrans05)

Ein besonderes Risiko besteht darin, dass das Verfahren in der Projektphase nicht hinreichend spezifiziert wird und die Projektumsetzung sich einer hinreichenden Kontrolle entzieht. (#RInt10)

Inwieweit eine **Kfz-Werkstatt** das CAN-Bus-Gerät vorsätzlich oder versehentlich erkennbar oder unerkennbar beschädigen oder die Daten verfälschen kann, ist nicht klar zu beurteilen. (#RInt04) Allerdings ist die OBD2-Schnittstelle so ausgelegt, dass auch schreibend auf den Datenbestand im Kfz zugegriffen werden kann und es sind rationale Motive denkbar, diese Daten zu ändern. Der schreibende Zugang zu den Kfz-Daten muss nicht zwingend im Kfz selber erfolgen, sondern kann während der Übermittlung an die Scorebox vorgenommen werden. Dann wäre ein Szenario wie Rabatt-Tuning durch ein spezielles Interface zwischen OBD2 und Scorebox denkbar: „Wir sorgen dafür, dass die Maximalgeschwindigkeit gemäß Datensatz nie überschritten wurde." Oder: „Wir sorgen dafür, dass bestimmte Fahrten nicht stattgefunden haben."

Ein (zur alleinigen Faktenklärung sicher nur unzureichender) Blick in die deutsche Wikipedia zur Klärung funktionaler Details der OBD2-Schnittstelle („On-Bord-Diagnose" (OBD) und „Diagnostic Trouble Code") [19] zeigt, dass ein Großteil der von dem Verfahren genutzten Kfz-Daten im Standarddatensatz nicht vorgesehen ist, und insofern herstellerspezifisch oder von den möglicherweise vorhandenen Sensoren in der Scorebox abgerufen werden müsste bzw. in Zusammenarbeit mit den Herstellern initiiert werden kann.

Die Schnittstelle ist weitgehend ungeschützt zugänglich. (#RInt04) Bislang jedenfalls sind die Adapter, Diagnosegeräte und PC-Software für jedermann zu geringen Preisen zugänglich. Dabei ist neben einem lesenden auch ein schreibender Zugriff auf den per OBD2-Schnittstelle zugänglichen Datenbestand möglich.[20] Dass personenbezogene Daten mit hohem Schutzbedarf in Kfz-Werkstätten verarbeitet werden, ist schon seit Jahren Fakt, hat bislang in der Praxis aber keine Auswirkungen auf die entsprechende IT gezeigt. Angesichts dieser Sachlage wird von einem hohen Risiko ausgegangen. Insofern darf der Schluss gezogen werden, dass eine beachtenswerte Eintrittswahrscheinlichkeit mit hohem Schadenspotential vorliegt.

Die Integrität der IT und Prozesse beim der **Funk-Tool sowie beim Funknetz-Provider**, also das Risiko einer Übermittlung falscher Daten und einer vorsätzlichen Fälschung im Kontext der Übertragung der Kfz-Daten per Funk ist gering, allein weil keine unmittelbare Motivation ersichtlich ist. Das Risiko, dass Daten von einem Kfz an ein falsches Rechenzentrum (Authentizität der Beteiligten) und von dort an eine falsche Versicherung übermittelt werden, besteht und ist zu beachten. (#RInt05)

Das Risiko, dass **die Cloud-Betreiber** die bei ihnen gespeicherten verschlüsselten Daten fälschen, ist auf Grund fehlender Anreize gering. Gleichwohl könnten die Administrationen der beteiligten Cloud-Betreiber Motive hegen, ihren Organisationen nachhaltig zu schaden, indem diese Kundendaten manipulieren oder löschen („revenge wipe"). Dieses Risiko ist zwar gegeben, die Eintrittswahrscheinlichkeit dürfte jedoch als gering eingestuft werden. (#RInt06)

Dass **Sicherheitsbehörden** auf die Kfz-Daten oder die Daten bzgl. des Fahrverhaltens zugreifen werden, darf für die Praxis als gesichert angenommen werden. (#RInt07) Der Zugriff kann dabei verdeckt

[19] https://de.wikipedia.org/wiki/On-Board-Diagnose … https://de.wikipedia.org/wiki/Diagnostic_Trouble_Code (Stand: 2017-0613)

[20] Onlineplattformen wie https://www.fahrzeuggeschichte.de/ machen die Ermittlung der Geschichte eines Kfz über die „Vehicle Identification Number" (VIN) für jedermann möglich. Ob darüber auch Angaben zu den Haltern eines Kfz ermittelbar sind, wäre zu prüfen.

und operativ mit geringem Aufwand durch Abgriff an der OBD2-Schnittstelle im Kfz erfolgen, grundsätzlich aber auch über die Daten in den Cloud-Speichern, über die Kfz-Hersteller, die Scorebox-Hersteller oder die Kfz-Werkstätte.

In Bezug auf Sicherstellung der **IT-Sicherheit** besteht bei allen beteiligten Organisationen ein zu beachtendes Risiko bzgl. der Sicherstellung der Integrität der Daten, IT-Systeme und Prozesse. Wie auch bei den IT-Administrationen der Organisationen sind Motive auf Seiten von Hackern denkbar, Datenbestände zu löschen, unbrauchbar zu machen oder zu fälschen. Hacker können von Konkurrenzunternehmen beauftragt sein, die Versicherung zu schädigen. Aber auch Erpressung der Versicherung wäre ein plausibles Motiv. (#RInt08)

Zudem sind Angriffe terroristischer Art denkbar, die zum Ziel haben die hinter dem Verfahren stehende Mathematik (Algorithmus) zu verfälschen und damit einerseits finanzielle Schäden zu verursachen und mittelbar das Vertrauen in gesellschaftlich anerkannte Prozesse zu erschüttern.[21] Andererseits könnte die Scorebox für Angriffe (DDoS-Angriff) auf kritische Infrastrukturen missbraucht werden, indem Sicherheitslücken gezielt ausfindig gemacht und die Box bspw. Teil eines Botnetzes wird. (#RInt09)

2.4.4. Vertraulichkeit

Das Vertraulichkeitsrisiko betrifft die unbefugte Kenntnisnahme der personenbezogenen Daten, sowohl der Kfz-Eigenschaften als auch des Fahrverhaltens. Wie schon bzgl. der Integrität so gilt auch bei der Vertraulichkeit, dass eine ersichtlich überbordende Komplexität bei der Sicherung einer vertraulichen Erhebung, Speicherung, Übermittlung und Berechnung von Daten und des dazu notwendigen Controllings der IT-Systeme und Prozesse einschließlich des Abschätzvorgangs selber in seiner Gänze dazu führt, dass ein generell hohes Risiko bzgl. der Vertraulichkeit der Daten für Betroffene besteht. (#RVert01)

Die Vertraulichkeit der Daten innerhalb der **Versicherung** wird weniger durch Verschlüsselung zu sichern sein, da die Daten nur unverschlüsselt inhaltlich verarbeitet werden können, sondern mehr durch ein differenziertes Rollen und Berechtigungskonzept. Das Risiko, dass Abteilungen der Insight AG unbefugt auf Daten anderer Abteilungen zugreifen, besteht. (#RVert02) Insbesondere ist es naheliegend, dass die Versicherungsmathematiker neuentwickelte Modelle auf den Produktivdaten rechnen wollen, weil diese maximal integer wären, dies aber allenfalls mit Einschränkungen rechtlich erlaubt wäre. Das Rechnen auf vollständigen oder teilweisen Kopien von Produktivdaten etwa im Kontext von Big Data ist gängige Praxis. (#RVert03) Die Eingriffsintensität und die Eingriffswahrscheinlichkeit sind hoch.

Im **Werkstatt-Kontext** können die Kfz-Daten an der Schnittstelle unverschlüsselt ausgelesen werden, und zwar unmittelbar bevor Daten in der Scorebox gespeichert werden. Abhängig von möglichen Vereinbarungen zwischen herstellergebundenen oder freien Werkstätten ist ein vollständiges Auslesen der Kfz-Speicher durch Werkstätten (wenn auch bevorzugt aus Gründen der technischen Wartung) vermutlich obligatorisch – schließlich haben die Kfz-Hersteller Kosten für die Installation, Speicherung und das Operating der Daten aufgewendet. Die Scorebox zwischenspeichert vermutlich auch solche Daten, die in der Kfz-IT nur temporär vorgehalten werden. Es besteht das Risiko, dass die Da-

[21] Versicherungen können als ein Teil kritischer Infrastrukturen gelten, siehe BSI: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/FinanzundVersicherungswesen/FinanzundVersicherungswesen_node.html

ten der Scorebox ausgelesen werden, insofern ist das Risiko unbefugter Kenntnisnahme der Daten hoch. (#RVert04) Hersteller und Werkstätten können jeweils eigene Verhaltensprofile ihrer Kunden erstellen und diese Daten an beliebige Interessenten verkaufen. Die Eingriffsintensität und die Eingriffswahrscheinlichkeit sind hoch.

Die **Funknetz-Provider und die Hersteller der Scorebox** haben zumindest Zugriff auf Metadaten der Beteiligten. (#RVert05) Vermutlich können sie selbst bei verschlüsselt vorliegenden Daten eigene Formen des Scorings und Profilings durchführen. Die Wahrscheinlichkeit, dass sie auf diese Daten zu eigenen Zwecken zugreifen ist hoch, und zwar gerade dann, wenn oder weil die Daten verschlüsselt vorliegen und es vordergründig so erscheint, als ob kein unmittelbarer Personenbezug gegeben ist. Ein Finanzierungsmodell könnte darin bestehen, dass die Funkeinheit kostenlos gestellt wird, wenn der Versicherungsnehmer Zugriff auf die Daten oder zumindest einen Teil der Daten, gewährt. Wenn die Daten vollständig verschlüsselt abgespeichert und verschlüsselt an das Funk-Tool gesendet werden, können diese Daten allerdings selbst bei zweifelhafter zusätzlicher Verschlüsselung auf Netzebene als vertraulich gelten – es sei denn, dass aufgrund mangelhafter IT-Sicherheit bei den Cloud-Betreibern wiederum andere Nutzer der Cloud sich Zugriff verschaffen können.[22]

Der zentrale **Cloud-Betreiber** hat Zugriff auf die Quelldaten des Kfz. Es besteht ein großes Risiko, dass der Cloud-Betreiber auf diese Daten zugreift. (#RVert06) Aufgrund der Wahl eines Cloud-Betreibers außerhalb der EU können keine verlässlichen vertraglichen Regelungen getroffen und es kann keine effektive Kontrolle des Auftragsnehmers durchgeführt werden. Auch aus Sicht der Versicherung besteht das Risiko, dass mit dem Zugänglichmachen der Kfz-Daten, deren exklusive Analyse ganz wesentlich zum Geschäftserfolg der Insight AG beiträgt, das Geschäftsgeheimnis der Versicherung bedroht ist.

Das Risiko bzgl. der Vertraulichkeit der IT von **Sicherheitsbehörden** ist hier kein Gegenstand der Betrachtung, da diese im Verantwortungsbereich der jeweiligen Behörde liegt. Allerdings besteht ein Risiko bzgl. der Sicherung der Vertraulichkeit bei der Übermittlung von Kfz- und Fahrdaten an eine Sicherheitsbehörde – auch abhängig von den Orten des Zugriffs. Die unmittelbare Direkterhebung der Kfz-Daten am Kfz eines Verdächtigen wäre, sofern ermittlungstaktisch möglich, grundrechtlich geboten. (#RVert07)

In Bezug auf Sicherstellung der **IT-Sicherheit** besteht bei allen beteiligten Organisationen ein zu beachtendes Risiko bzgl. der Sicherstellung der Vertraulichkeit der Daten. Wie auch bei den IT-Administrationen der Organisationen sind Motive auf Seiten von Crackern denkbar auf Roh-Datenbestände zuzugreifen, um die Versicherung damit zu erpressen. Weil die Kfz- und Fahrdaten den Kern des Geschäftsmodells der Versicherung darstellen, darf man davon ausgehen, dass die Versicherung zumindest die üblichen Schutzmaßnahmen ergreift. (#RVert08)

2.4.5. Transparenz

Übergreifend ist festzustellen, dass es im geschilderten Modellfall an Transparenz bzgl. der Rechtsgrundlagen sowie sehr vieler funktionaler und sicherheitstechnischer Verfahrenseigenschaften, die

[22] Die Verwendung einer zweifelhaften Verschlüsselungsmethode, etwa aus Kostenspargründen, erscheint uns unrealistisch bzw. praxisfremd, weil es inzwischen einfacher und billiger ist, die vorgesehenen Standardverschlüsselungsalgorithmen der Standardprogrammiersprachen zu nutzen als eine eigene „Verschlüsselung“ zu entwickeln, von der Programmierer wissen, dass dies Argwohn hervorrufen wird. Wenn trotzdem eine selbstgestrickte Verschlüsselung genutzt wird, dann liegt das Motiv auf der Hand, dass diese Verschlüsselung gebrochen werden soll. Kosten kann jedoch ein korrektes Handling der Zertifkate verursachen, das bei „hohem Schutzbedarf“ unabdingbar ist.

von jeder beteiligten Organisation, im Auftrag der Versicherung, zu erfüllen sind, fehlt. Das Risiko ist insofern groß, dass bei unklarer Rechtslage nicht der tatsächliche Satz an Kfz-Daten, der aus den Kfz ausgelesen werden kann oder ausgelesen wird, bekannt ist. (#RTrans01)

Ebenso wenig ist erkennbar, welche IT und Prozesse bei den Organisationen, die beteiligt wären, zum Einsatz kommt und welche Schutzmaßnahmen diese dann umsetzen bzw. umsetzen können. Das Risiko der Intransparenz des Verfahrens im Hinblick auf die Bestimmung, welche Organisationen und Personen Zugriff auf die Daten oder auf die IT zur Berechnung eines Scores haben und bzgl. der Wirksamkeit etwaig zum Einsatz kommender Schutzmaßnahmen ist insofern groß. (#RTrans02)

Transparenz muss zudem bzgl. der Rechte und Pflichten bestehen, die die beteiligten Organisationen (Kfz-Werkstätten, Scorebox-Hersteller inkl. Funkmodul-Provider, Cloud-Betreiber) gegenüber der Versicherung haben. Es besteht das Risiko, dass der Leistungsumfang, der seitens der Organisationen zu erbringen bzw. welche Art der Datenverarbeitungen auszuschließen ist, nicht hinreichend definiert ist und dass nicht alle Schutzmaßnahmen der IT-Sicherheit erfasst werden. (#RTrans03)

Ein weiteres Transparenzproblem besteht darin, dass Hacker- und/oder Sicherheitsbehörden direkt auf die Kfz-Daten bzw. die Daten bei den Datenverarbeitern oder auch auf die Roh- und Profiling-Daten bei der Versicherung zugreifen, ohne dass solche Zugriffe, insbesondere die von Sicherheitsbehörden, für die betroffene Person erkennbar sind (#RTrans05).

Es besteht das Risiko, dass der Kfz-Halter darüber, dass eine automatisierte Entscheidungsfindung und Profiling vorliegen, nicht informiert wird und die Logik, Tragweite und die angestrebten Auswirkungen der Entscheidung deshalb nicht überblicken kann. (#RTrans06).

2.4.6. Nichtverkettung

Das Verkettungsrisiko umfasst die zweckentfremdende Nutzung des Verfahrens bzw. der personenbezogenen Daten des Verfahrens. Zweckentfremdenden Zugriff kann durch die Werkstatt erfolgen, die eine Scorebox einbaut bzw. ausbaut, durch den Funknetz-Provider, der die Daten nur weiterleiten darf, durch den Funk-Tool-Hersteller, darf die Daten aus der Scorebox nur weiterleiten darf, durch die Cloud-Betreiber, die die Daten nur entgegennehmen und nur für eine bestimmte Stelle abrufbar speichern dürfen. Die Versicherung darf die Daten nur für den dem Kunden ausgewiesenen Zweck verarbeiten. Wirklich berechtigt zur Verarbeitung der Daten im engen Sinne einer befugten Auswertung und Berechnung ist einzig die Versicherung, die deswegen im Grundsatz Zugriff auf alle erforderlichen Daten haben darf. Wenn die anderen beteiligten Organisationen die Daten zu anderen als den vertraglich bestimmten, die Datenschutzanforderungen berücksichtigenden, Zwecken verwerten, dann ist das ein unbefugter Zugriff und damit ein Vertraulichkeitsverstoß. Das eigentliche Verkettungsrisiko besteht deshalb bei der Versicherung.

Die **Versicherung** hat ein strukturelles Interesse, das ohnehin schon differenzierte Geschäftsmodell zur Ermittlung eines angemessenen Versicherungsbeitrags beständig weiter zu differenzieren. Dafür müssen immer neue Faktoren zur Risikobestimmung oder theoretisch gestützte zusätzliche Annahmen über das Fahrverhalten aus den gegebenen Kfz-Daten entwickelt werden. Dadurch wird im Ergebnis nicht nur das Verhalten des Kfz-Halter immer genauer erfasst und im Nachhinein analysierbar sondern mehr noch auch das Handeln der Betroffenen zunehmend zuverlässiger prognostizierbar und steuerbar. (#RN01) Insofern besteht ein hohes Risiko, dass die Versicherung die Genauigkeit der Verhaltenskontrolle beständig weiter ausbaut, auch mit dem Seitenblick auf das Abwehren von Regulationsansprüchen. Die tatsächlichen Fahrer, Zweitfahrer und Beifahrer eindeutig zu identifizieren, ist

ein weiterer denklogisch naheliegender nächster Schritt zur Verbesserung des Fahrer-Scores. Weil diese personenbezogenen Daten einen hohen Wert innehaben, droht notorisch die Weitergabe von Daten an andere Organisationen, die dann andere Zwecke verfolgen.

Die Rohdaten aus den Kfz werden gemäß Modellfall drei Jahre aufbewahrt, sie sollen durch Entfernen der Fahrgestellnummer anonymisiert werden um dann für Forschung und Entwicklung unbegrenzt zur Verfügung zu stehen. Eine ausreichende Anonymisierung ist nicht allein aufgrund des Entfernens der Fahrgestellnummer zu erreichen, denn das umfangreiche Bewegungsprofil des Fahrers kann durch Zusammenführen mit anderen Datensätzen leicht wieder einer bestimmten Person zugeordnet werden. (#RN02) So führt schon der Vergleich eines „anonymisierten" Datensatzes (älter als 3 Jahre) mit aktuellen Bewegungsprofilen mit hoher Wahrscheinlichkeit zur De-Anonymisierung. Zudem macht die in das Kfz eingebaute SIM-Karte das Fahrzeug und damit auch den Fahrer jederzeit identifizierbar, da nicht davon auszugehen ist, dass diese nach einer bestimmten Zeit ausgewechselt wird. (#RN03)

Ein weiterer Aspekt ist die Verkettung mit Daten anderer Telematik-Versicherter. Diese Verkettung wird als Funktionalität explizit erwähnt und wirkt sich direkt auf den Scorewert aus. Inwiefern aus den vorhandenen Daten auf ein Straßenrennen geschlossen werden kann, wie im Modellfall als errechenbar angenommen wird, ist fraglich, denn es könnte sich auch um reguläre Überholmanöver handeln oder es wird nur der Eindruck eines Rennens erweckt, obwohl die zu dem Zeitpunkt herrschende Verkehrssituation eine untypische Fahrweise verlangte. (#RN04)

Nicht geklärt ist außerdem, was mit der Zusatztechnik passiert, wenn ein Fahrzeugverkauf stattfindet bzw. es sich beim Kfz um einen Leasingrückläufer handelt. (#RN05)

Die Möglichkeiten der Verkettung sind – betrachtet man die Vielfalt der erhobenen Daten – enorm. Bereits vor der Anonymisierung bzw. während des Scorings sollen Big Data- Anwendungen eingesetzt werden. Das Risiko, dass diese Daten zur Erstellung bzw. Vervollständigung eines Persönlichkeitsprofils verwendet werden, ist entsprechend hoch.

2.4.7. Intervenierbarkeit

Das Interventionsrisiko bezeichnet zwei Aspekte: Zum einen, dass ein Verfahren die Betroffenenrechte auf Berichtigung von Daten, Widerruf von Einwilligungen und Kündigung von Verträgen, Löschen von Daten und die Nachweise hierüber nicht hinreichend wirksam umsetzt (#RIv01). Zum zweiten beschreibt es, dass eine Organisation nicht hinreichend in der Lage ist, das Verfahren transparent, zweckgemäß und integer zu ändern, weil dies bspw. rechtlich gefordert oder technisch notwendig ist („Changemanagement"). Auf Änderungsanforderungen zu reagieren und diese intern umsetzen zu können, ist ein Aspekt, der alle beteiligten Organisationen betrifft und ein wesentlicher Prüfaspekt eines übergreifenden Datenschutzmanagements ist. (#RIv02).

Für den Versicherungsnehmer ist nicht erkennbar, wann welches Modell zur Berechnung des Scorewertes verwendet wurde. Da selbstlernende Algorithmen sich über den Versicherungszeitraum bzw. den Berechnungszeitraum hinweg verändern, kann ein und dasselbe Verhalten zu unterschiedlichen Scorewerten führen. Im Verfahren ist jedoch keine Möglichkeit vorgesehen, die eine Überprüfung des tagesaktuellen Scorewertes erlaubt. Dem Fahrer wird damit keine Möglichkeit gegeben, einen ungünstigen Scorewert wahrzunehmen und ggf. bei der Versicherung ein fehlerhaftes Berechnungsmodell zu beanstanden.

Für den Fahrer ist bei keiner der beteiligten Organisationen die Möglichkeit vorgesehen, die Datenverarbeitung zu kontrollieren und ggf. Daten zu korrigieren – z.B. falls er nicht selbst gefahren ist – oder zu stoppen. Das sich hieraus ergebende Risiko einer unumkehrbaren Fehlentscheidung zu Lasten des Fahrers auch aufgrund der ausdrücklich untersagten (!) Verarbeitung besonderer Kategorien personenbezogener Daten, wie der ethnischen Herkunft, ist nicht zu rechtfertigen. (#RIv03) Es wird auch nicht erwähnt, ob die Daten aus den Vorjahren in den aktuellen Score einfließen oder ob der Algorithmus letztendlich zwischen einzelnen Fahrern unterscheiden kann bzw. inwieweit die Versicherung bei einem selbstlernenden Algorithmus überhaupt Kontrolle über die Berechnung des Scorewertes behält und unerwünschte Effekte „herausrechnen“ kann.

3. Maßnahmenbestimmung

Die nachfolgende Auflistung von operativen Anforderungen für den Modell-Fall eines Pay-as-you-drive-Verfahrens der Versicherung „Insight AG“ erfolgt anhand des oben ausgewiesenen Standard-DSFA-Prozessablaufs. Rechtlich problematische Nebenbedingungen dieses Modellfalls werden, zum Zweck des Vergleichs von DSFA-Methoden, akzeptiert. Gemäß SDM-Methodik wäre zunächst die rechtliche Prüfung des Verfahrens abzuwarten, bevor die SDM-Methodik genutzt werden kann, um Maßnahmen auszuwählen, zu dimensionieren, zu überwachen und zuletzt die Überwachungsergebnisse einer juristischen Beurteilung zugänglich zu machen. Aufgrund des Prüfungsergebnisses sähe sich eine Projektgruppe der Modell-Versicherung, deren Rolle die Autoren dieses Textes einnehmen, aufgefordert, die Funktionalitäten des Verfahrens bzw. dessen Spezifikationen zu ändern und nicht, so wie hier, bestimmte Nebenbedingungen zu akzeptieren und nur noch die Installation einiger Schutzmaßnahmen zu empfehlen.

Konkrete Umsetzungsempfehlungen der nachfolgenden Anforderungen sind künftig den SDM-Bausteinen zu entnehmen. Bislang wurden SDM-Bausteine mit konkreten Umsetzungsempfehlungen erstellt, aber noch nicht veröffentlicht. Solange keine SDM-Bausteine zur Verfügung gestellt wurden, sollten die generischen Maßnahmen aus Kapitel 7 des SDM-Methodik-Handbuches herangezogen werden, die anhand von Orientierungshilfen der Datenschutzaufsichtsbehörden[23] und/oder entsprechenden Umsetzungsempfehlungen nach IT-Grundschutz des BSI[24] weiter konkretisiert werden können.

3.1 Identifikation/ Auswahl von Maßnahmen

Ausgangspunkt zur Identifikation und Bestimmung von erforderlichen Schutzmaßnahmen ist das Verfahren als vollständige Prozesskette, das die Versicherung „Insight AG“ zu betreiben plant.

Bevor operative Anforderungen zu benennen sind, sind zunächst immer rechtliche Anforderungen zu erfüllen. Mit allen Beteiligten sind spezifische Verträge zu schließen. Jeder Vertrag sollte – strukturiert nach den Gewährleistungszielen – Regelungen bezüglich zu installierender Schutzmaßmaßnahmen, zur Überwachung von Funktionen und Schutzmaßnahmen sowie Regelungen zu Konfliktlösungen enthalten. Diese im Vertrag aufzugreifenden Aspekte werden nachfolgend angesprochen.

Die größte rechtliche Herausforderung dürfte die rechtliche Bindung von Werkstätten seitens der Versicherung sein. Ein praktikabler Weg dürfte dabei sein festzulegen, dass die Scorebox in der Regel nur von Hersteller-gebundenen Vertragswerkstätten eingebaut werden darf. Dadurch können der Einbau, Umbau und Ausbau unter Rückgriff auf kontrollierbare IT-Systeme (Protokollierung, Quittierung) anhand standardisierter, überwachbarer Prozesse erfolgen. Hersteller-ungebundene freie Werkstätten können, soweit sie die wesentlichen Eigenschaften zur Einhaltung der Anforderungen nachweisen, von der Versicherung eine Einbau-/Umbau-/Ausbaulizenz erhalten. Eine weitere Variante wäre, dass eine beliebige Werkstatt eine Scorebox einbauen kann, der Einbau in das Kfz jedoch anschließend von einer zertifizierten Prüfinstanz auditiert werden muss.

In Bezug auf die operative Durchsetzung der Datenschutzanforderungen sind konsequent alle Schutzmaßnahmen, die das SDM als Referenzmaßnahmen für die sieben Gewährleistungsziele auflis-

[23] Siehe den Katalog der Orientierungshilfen unter https://www.datenschutz-mv.de/datenschutz/publikationen/download.html
[24] Einstiegsseite zum IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

tet, über die gesamte Prozesskette hinweg, vollständig umzusetzen, denn es handelt sich um ein personenbezogenes Verfahren mit hohem Schutzbedarf. Aufgrund dessen darf keines der Gewährleistungsziele, die vollständig in Artikel 5 der DSGVO verankert sind, unbeachtet bleiben. Abweichungen von den Referenzmaßnahmen, die zu nutzen das SDM empfiehlt, wären begründungsbedürftig und die funktionale Äquivalenz von Ersatzmaßnahmen zu diesen Maßnahmen wäre nachzuweisen.

Für den Modellfall nimmt die Projektgruppe an, dass zur Spezifikation der operativen Anforderungen und Schutzmaßnahmen drei operative Bereiche getrennt zu betrachten sind:

a) Die IT-Infrastruktur der Versicherung. Das Pay-as-you-drive-Verfahren der Versicherung setzt, als ein Verfahren neben anderen, auf einer bestehenden IT-Infrastruktur der Versicherung auf. Ein anderes Verfahren umfasste bspw. all diejenigen Prozesse, die im Zusammenhang mit einer anderen Versicherungsart stehen.
b) Das Verfahren Pay-as-you-drive selbst mit operativen Anforderungen unmittelbar aus diesem Verfahren innerhalb der Versicherung.
c) Die operativen Verfahrensbestandteile, die die Dienstleister für die Versicherung speziell für dieses Verfahren erbringen.

Für die Bearbeitung des Modellfalls werden insofern nur die Bereiche b) und c) betrachtet. Für die vorliegende DSFA muss vorausgesetzt werden, dass die Infrastruktur, die vom Verfahren genutzt wird, rechtskonform sowohl in Bezug auf den operativen Datenschutz als auch regelkonform in Bezug zur IT-Sicherheit, z.B. nach IT-Grundschutz betrieben werden kann. Auch wird unterstellt, dass die Versicherung sowohl über ein Datenschutzmanagement, etwa auf der Basis des SDM, als auch ein Sicherheitsmanagement, etwa nach ISO27001 oder IT-Grundschutz des BSI, in Bezug auf diese Infrastruktur verfügt. Konkret bedeutet das, dass die Infrastruktur mit hinreichender funktionaler Redundanz (Verträge mit IT-Dienstleistern, Backup, Aufbewahrung) ausgestattet ist, dass Maßnahmen zur Sicherung der Integrität der Datenbestände (Zertifikate, Standardisierung, Überprüfung von Prozessen, gehärtete IT-Systeme) ergriffen, alle Funktionen und Schutzmaßnahmen überprüfbar spezifiziert, dokumentiert und protokolliert werden und mit hinreichend voneinander separierten Systemen und Prozessen, unter Durchsetzung der Betroffenenrechte bis in die allgemeine IT-Infrastruktur hinein ausgeführt werden. Nur dann kann auch das geplante Verfahren Pay-as-you-drive überhaupt rechtskonform betrieben werden.

3.1.1. Datenminimierung

Das Gewährleistungsziel der Datenminimierung kann maßgeblich durch Gestaltung des Verfahrens auf Seiten der **Versicherung** erreicht werden. Der Versuch einer zweistufigen Datenminimierung muss in einem realen Fall ganz am Anfang der Projektierung eines Verfahrens stehen.

Gesetzlich ist Datenminimierung gefordert, was bei einem rechtlich legitimierten personenbezogenen Verfahren konkret zur Reduzierung erfasster Attribute betroffener Personen, die Reduzierung der Möglichkeiten zur Kenntnisnahme vorhandener Daten und die Reduzierung der Verarbeitungsprozesse führen muss. Das läuft allerdings konträr zum Wesen der Geschäftsinteressen der „Insight AG“, nämlich beständig weitere Kfz-Eigenschaften zu erheben und immer riskantere Personenmodelle aus den Korrelationen bereits vorhandener oder neuer Kfz- und Kontextdaten zu erstellen. Die Implementierungen von Sperr- und Löschroutinen sowie die Pseudonymisierung und Anonymisierung der Verhaltensdaten zur Risikoberechnung sind bereits angesprochen worden.

Des Weiteren muss geprüft werden, ob die hohe Auflösung einer sekündlichen Erfassung der Kfz-Daten erforderlich ist, um eine korrekte Klassifikation des Risikotyps vorzunehmen. Bei der Modellierung der Datenklassen ist darauf zu achten, dass für eine gerade noch ausreichende Diskriminierung nur das minimal notwendige Set an Kfz-Daten genutzt wird, um den Grundrechtseingriff, der absehbar auf eine Vollüberwachung der Handlungen eines Kfz-Fahrers hinausläuft, so gering wie möglich auszugestalten. Es ist in diesem Zusammenhang damit zu rechnen, dass zur Fahrermodellierung auch Sensoren zur mentalen Überwachung des Fahrers (Müdigkeit, mangelnde Fokussierungen) installiert werden.

Die **Kfz-Werkstätten** müssen sicherstellen, dass im Kontext des Einbaus / Umbaus / Ausbaus der Scorebox und dem Kontakt zum Kfz-Halter oder Kfz-Fahrer und der Versicherung keine weiteren Daten an die Versicherung übermittelt werden (etwa zu Eigenschaften des Kfz-Halters/Fahrers) oder zum allgemeinen Zustand des Fahrzeugs.

Der **Scoreboxhersteller** muss sicherstellen und nachweisen können, dass die Scorebox keinerlei Daten über diejenigen hinaus erzeugt und übermittelt, die von der Versicherung zur Risikobestimmung als erforderlich angefordert werden.

Die **Cloud-Betreiber** müssen sicherstellen und nachweisen können, dass diese keinerlei zusätzlichen Daten über die bei ihnen gespeicherten Daten hinaus speichern und übermitteln.

Zu den Anforderungen der Beachtung der Datenminimierung sowie der daraus folgenden funktionalen und sicherheitstechnischen Umsetzungen bei den **Sicherheitsbehörden**, muss hier keine Aussage gemacht werden.

Als Empfehlungen zur Umsetzung von Anforderungen an die Datenminimierung auf der Ebene einzelner Maßnahmen bei den verschiedenen Organisationen liegen im Kontext des SDM bislang keine direkt darauf Bezug nehmenden Textentwürfe vor. Allerdings werden Anforderungen an die operative Seite der Durchsetzung der Datenminimierung im Wesentlichen mit den Bausteinen zum Umsetzung der Nichtverkettung bereits erfüllt.

3.1.2. Sicherung der Verfügbarkeit

Die Sicherung der Verfügbarkeit des Verfahrens geschieht auf Seiten der **Versicherung** im Rahmen der vermutlich bereits ohnehin verwendeten Lösungen für die gesamte IT-Infrastruktur. Das bedeutet konkret, dass Prozesse bereitstehen müssen, wonach die Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts gesichert sind. Es bedeutet Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt), die Dokumentation der Syntax der Daten, Redundanzen für Hard- und Software sowie Infrastruktur einzubeziehen sowie über Reparaturstrategien und Ausweichprozesse zu verfügen und nicht zuletzt Vertretungen für abwesende Mitarbeiter zu regeln. Wegen des hohen Schutzbedarfs sind alle diese Maßnahmen besonders sorgfältig zu planen, im laufenden Betrieb besonders sorgfältig zu sichern und regelmäßig zu überwachen. (#BRVerf01)

Die Versicherung muss zudem Sorge dafür tragen, dass sie die Daten zu einem Versicherungsnehmer bzw. Kfz-Halter zusammentragen kann, um das Recht auf Datenübertragbarkeit (Art. 20 Abs. 1 DSGVO) operativ einlösen zu können (#BRVErf03). Wie umfänglich dieser Datensatz ist, ob auch die Kfz-Quelldaten enthalten sein müssen, dagegen keinerlei errechnete Profiling- und Scoredaten, muss rechtlich geprüft werden.

Die bislang nicht veröffentlichten SDM-Bausteine „Datensicherung und Wiederherstellung“ und „Aufbewahrung“ enthalten konkrete Umsetzungsempfehlungen.

Bei den **Kfz-Werkstätten** sind in Bezug auf die Sicherung der Verfügbarkeit des Verfahrens keine besonderen Maßnahmen vorzusehen. Weil eine Werkstatt mit dem Ein-, Um- und Ausbau der Scoreboxen Geld verdient, wird diese über die notwendigen Redundanzen auf der operativen Ebene verfügen.

Bei der **Scorebox selbst und dem Funknetz-Provider** sind ebenfalls keine besonderen Maßnahmen zur Steigerung der Redundanz vorzusehen. Zur Kompensation von Funklöchern muss der Speicher Funklöcher beachten und der Datenzwischenspeicher hinreichend groß bemessen sein, so dass zwischengespeicherte Daten gesendet werden, sobald wieder Funkkontakt besteht. Beim Ausfall der Scorebox muss der Kfz-Fahrer einen Hinweis erhalten, dass diese repariert werden muss. Ausfallzeiten durch eine defekte Scorebox sollten bis zu einem gewissen Grad nicht zulasten des Kfz-Halters gehen. Dies sollte vertraglich dem Kfz-Versicherten zugesichert werden. (#BRSB01)

In Bezug zum **Cloud-Betreiber** ist bereits im Modellfall die Sicherung der Verfügbarkeit durch die Nutzung einer externen Fallback-Cloud vorgesehen. (#BRCVerf03)

Als Empfehlungen zur Umsetzung von Verfügbarkeitsanforderungen auf der Ebene einzelner Maßnahmen liegen die, im Kontext der Unterarbeitsgruppe „SDM“ erarbeiteten aber noch nicht publizierten, Texte zu „Aufbewahrung“ und „Backup“ vor.

3.1.3 Sicherung der Integrität

Die **Versicherung** muss die Integrität des Verfahrens als Ganzes sichern. Das bedeutet, dass Schreib- und Änderungsrechte von Mitarbeitern unterschiedlicher Abteilungen im Rahmen eines dokumentierten Rollen- und Berechtigungskonzept zu regeln sind. Wenn Daten übertragen werden, insbesondere von und zu anderen Organisationen bzw. wenn Daten von anderen Organisationen übermittelt werden, sind Prüfsummen, elektronische Siegel und Signaturen in den Datenverarbeitungsprozessen gemäß einem Kryptokonzepts zu nutzen. Dieses Kryptokonzept muss Aspekte aufgreifen, die unter dem Stichwort „Public-Key-Infrastructure“ thematisiert werden und vor allem das Zertifikate- bzw. Schlüsselmanagement (wie Ausstellen, Verteilen, Verwalten, Benachrichtigen über, Zurückziehen und Löschen von Zertifikaten) umfassen, insbesondere für die operativen Komponenten, bei denen Daten per Internet übermittelt werden. Zur Integritätssicherung zählen des Weiteren Prozesse zur Aufrechterhaltung der Aktualität von Daten über die gesamte Prozesskette hinweg. Außerdem ist für alle Prozesse (bspw. der regelmäßigen Datenübermittlung, der Überwachung, der Dokumentation, der Behebung von Fehlern) zu definieren, innerhalb welcher Breite diese schwanken dürfen, damit diese als „integer“ gelten können. Es sind regelmäßige Tests durchzuführen, bei denen diese Prozesse auch in Ausnahmezustände versetzt, um die Qualität von Reparaturprozessen beurteilen zu können. (#BRInt01).

Die Versicherung sollte zudem ein Audit der IT-Sicherheit durchlaufen (#BRInt02).

Zur Sicherung der Integrität des Verfahrens als solches muss die Versicherung über ein Datenschutzmanagementsystem verfügen, das einer kontinuierlichen Fortschreibung und Verbesserung gem. Deming-Zyklus unterliegt. Insbesondere sind die Dienstleister, die im Modus der ADV agieren, anzuleiten, indem erstens die Inhalte und die dafür zu nutzenden IT-Anwendungen und Prozesse definiert werden. Zweitens ist die Ausführung der Kontrollen der Dienstleister durch die Versicherung festzu-

legen inklusive drittens der Definition der Prozesse, mit denen Konfliktfälle transparent, integer, zweckgemäß gelöst werden sollen (#BRInt03).

Eine besondere Beachtung erfordert die Umsetzung der Anforderung, dass Datenschutzvorfälle an die Aufsichtsbehörden zu melden sind. Dafür sind seitens der Versicherung erstens Datenschutzvorfälle, die auch die Auftragnehmer umfassen, zu typisieren und zweitens Meldeprozesse an die Meldebehörden vorzusehen und zu testen. (#BRInt13).

Die **Kfz-Werkstätten** wurden in der Risikoanalyse als das in der Praxis vermutlich größte operative Risiko der Zwecküberdehnung oder des unbefugten Zugriffs auf die Scorebox ausgemacht. Es sind Motive denkbar und operative Ressource vorhanden, um Kfz-Daten zu verändern, sei es zugunsten von Kfz-Haltern, zugunsten der Versicherung oder auch auf Geheiß von Sicherheitsbehörden mittels forensisch ungesicherten Auslesens oder Abspeicherns, entweder an der OBD2-Schnittstelle oder grundsätzlich auch über andere Schnittstellen (bspw. für Updates der Software) der Scorebox.

Bei Werkstattaufenthalten bzw. beim TÜV sollten die OBD2-Schnittstelle und die Scorebox grundsätzlich auf fehlerfreie Funktionen getestet und dies quittiert werden. (#BRW01) Der Prozess des Auslesens von Daten mit Bezug zur Scorebox in der Werkstatt sollte unterbunden oder wenn nicht möglich, dann vollständig protokolliert werden. (#BRW02)

Die Scorebox sollte als Maßnahme eines elementaren IT-Sicherheitsschutz in einem abgeschlossen Bereich des Kfz eingebaut sein. (#BRS01)

In der Scorebox sollte ein spezieller Sensor vorgesehen werden, der die Kopplung der Scorebox mit dem OBD2-Bus protokolliert und seitens der Werkstatt, die diese Kopplungen vornimmt, eine Authentisierung der Werkstatt verlangt. So lassen sich in der Scorebox Authentisierungsschlüssel lizensierter Werkstätten hinterlegen, die sicherstellen, dass nur autorisierte Werkstätten den OBD2-Bus mit einer Scorebox verbinden. Jeder (Ab-)Koppelvorgang sollte dann protokolliert werden und Teil des Datensatzes sein, der der Versicherung zugeschickt wird (welche Instanz hat welche Aktivitäten zu welchen Zeitpunkt durchgeführt?). Es ist zudem zu prüfen ob ein Werkstatt- und Scorebox-spezifischer Code eingegeben werden sollte, mit dem die Box nach dem Einbau durch die Werkstatt erst scharf gestellt werden kann. Dass es keinen physikalischen Zugang auf die Inhalte der Scorebox seitens der Werkstatt geben kann, ist durch Verplombung sicherzustellen. Die Programmierung und Versiegelung der Scoreboxen wäre durch den Scorebox-Hersteller sicherzustellen. Hier gilt es insbesondere zu verhindern, dass Werkstätten auf relevante Kfz-Daten zur Score-Berechnung schreibend zugreifen können. (#BRW03, #BRW04)

Die Vertragswerkstätten sind aufzufordern für die Versicherung einen Standard-Prozess zu entwickeln und umzusetzen, wie die Scorebox gesichert eingebaut, umgebaut/updatet und ausgebaut werden kann und dieser Prozess vollständig überprüfbar protokolliert wird, ohne dass Mitarbeiter von Kfz-Werkstätten Kfz-Daten unbefugt zur Kenntnis nehmen, woanders als auf vorher definierten Speichern abspeichern und verändern oder transferieren können. (#BRW05)

Der **Scorebox-Hersteller** muss die Scoreboxen eindeutig voneinander unterscheiden können.

Der Funktionsumfang der Scorebox muss, auch unter Rückgriff auf diesen DSFA-Bericht, im Hinblick auf IT-Sicherheit und operativen Datenschutz spezifiziert und dann von einer externen Testinstanz überprüft bzw. auditiert werden. (#BRHS01)

Wenn die Scorebox in der Funktion eines Kfz-Daten zwischenlagernden Proxies zur Funkübertragung eingesetzt wird, dann ist diese Funktionalität relativ leicht zu überprüfen.

Die Scorebox sollte darüber hinaus als Vertrauensanker dienen, um eine Ende-zu-Ende-Sicherheit zumindest ab der Scorebox zu erlangen, indem Datenpakete, die in der Scorebox erzeugt werden, signiert werden, so dass auf Seiten der Versicherung überprüft werden kann, ob die Kfz-Daten entlang der gesamten Prozesskette integer übertragen wurden. Insofern muss das Protokoll, der zu übertragenden Nutzdaten und Metadaten, einschließlich der Prüfungen auf Integrität, definiert werden. Diese Maßnahme behebt die Vertraulichkeits- und Verkettungsrisiken (#BRP02, #BRP03, #BRP04, #BRW02, #RW03).

Getestet bzw. auditiert werden muss darüber hinaus, ob der Scorebox-Hersteller unberechtigt weitere Daten speichern lässt oder bereits übertragende Daten nicht gelöscht sowie ob eine anderweitige Verarbeitung oder auch eine Übermittlung von Daten stattfindet. Auch dies setzt eine Auditierung speziell der Scorebox, entweder initiiert durch die Versicherung oder durch eine vertrauenswürdige Stelle im Rahmen einer Standardisierung solcher Scoreboxen, voraus (#BRInt02).

Die vorstehenden Maßnahmen setzen voraus, dass jede Scorebox eindeutig identifizierbar und adressierbar sein muss. Die Scorebox-Identnummer muss eindeutig an die Kfz-Fahrzeugnummer gekoppelt sein. (#BRH02)

Eine Integritätssicherung der zu übertragenden Daten in der Scorebox bietet Schutz vor Integritätsrisiken, die durch den **Funknetz-Provider** entstehen können. Zusätzlich sollte eine Transport-Sicherung vorgesehen sein, um die Authentizität der beteiligten Instanzen (Scorebox, Provider, Cloud-Speicher) sicherzustellen. (#BRP02, #BRP03, #BRP04).

Es muss qua Authentisierungsmaßnahmen sichergestellt werden, dass die Daten aus der Scorebox beim richtigen **Cloud-Betreibers** landen. (#BRC01)

Um die Kfz-Daten vor **Hacking-Angriffen**, bei denen Daten eingesehen, verändert und/oder gelöscht werden können, zu sichern, wäre eine Risikoanalyse speziell zur IT-Sicherheit entlang der Prozesskette durchzuführen. Die OBD2-Schnittstelle ist konstruktionsbedingt leicht zugänglich. Sobald die Daten die Scorebox erreichen, sollten diese signiert oder mit einer (kryptographischen) Prüfsumme versehen werden. (#BRH01) Derartig behandelte Daten böten auch Integritätsschutz während der Funkübermittlung, während der Speicherdauer in den Cloud-Speichern und bei der nochmaligen Übermittlung aus der Cloud an die IT der Versicherung. Bei der Scorebox muss sichergestellt werden, dass außer dem definierten Input aus der OBD2-Schnittstelle und dem definierten Output per Funk-Tool keine weiteren, außerhalb der Scorebox zugänglichen, Schnittstellen bereitstehen. Auf die Übermittlung von Daten über eine weitere Bluetooth-Schnittstelle an eine App sollte verzichtet werden (#BRM01). Die notwendige Wartung speziell der Scorebox wäre relativ leicht und sicher über einen Schnittstelle im Scorebox-Inneren umsetzbar, ob ein zertifikatgesichertes Einspielen von Updates online über eine Funkverbindung sicher möglich ist, wäre eigens zu prüfen. Neben der physikalischen Sicherung sollte die Wartungsschnittstelle zusätzlich über einen Authentisierungsvorgang in Verbindung mit einer Protokollierung der Aktivitäten an dieser Schnittstelle verfügen. Die Überprüfung der Protokolle sollte in hochauflösender Form durch die Versicherung sowie in einer aggregierten Form auch durch den Kfz-Halter geschehen.

Als Empfehlungen zur Umsetzung von Integritätsanforderungen auf der Ebene einzelner Maßnahmen liegen die, im Kontext der Unterarbeitsgruppe „SDM“ erarbeiteten aber noch nicht publizierten, Texte zu „Ticketsystem“ und „Administrationsplattform“ vor.

3.1.4. Sicherung der Vertraulichkeit

Sobald die Daten die Scorebox erreichen, sollten diese in der Box signiert und verschlüsselt zwischengespeichert und die Ausgangsdaten gleichzeitig gelöscht/gewiped werden. (#BRH01)

Die **Versicherung** muss die Vertraulichkeit des Verfahrens für die gesamte Prozesskette, und insbesondere auch bei der eigenen IT vor Ort, im unmittelbaren Zugriff der Versicherung, sicherstellen. Das bedeutet konkretisiert, im Rollen- und Berechtigungskonzept muss entsprechend der Erforderlichkeit der Zugriff auf die Daten (#BRV08, #BRV02, #BRV06, #BRV07, #BRV08) und dazu ein sicheres Authentisierungsverfahren eingerichtet werden. Die Zuordnung des Personals muss auf solche eingegrenzt werden, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind und keine Interessenskonflikte bei der Ausübung ihrer Tätigkeiten aufweisen. Die Nutzung zugelassener Ressourcen, insbesondere der Kommunikationskanäle speziell mit Bezug zum Zwischenspeicher in der Cloud, muss festgelegt und überwacht werden. Die Abteilung, die Gebäude und Räume, die von den Verfahrensbeteiligten genutzt werden, müssen definiert und deren Nutzung überwacht sein. Die organisatorischen Abläufe, z.B. wann welcher interne oder externe Mitarbeiter zu welchem Zweck zu beteiligen ist, müssen spezifiziert und der Betrieb überwacht werden. Es sind Regelungen zu treffen, die alle am Verfahren Beteiligten auf die Einhaltung der Vertraulichkeits- und Verschwiegenheitsvereinbarungen verpflichten. Daten sind, bei hohem Schutzbedarf zu verschlüsseln, sowohl wenn sie gespeichert als auch wenn sie transferiert werden. Die sichere Verwaltung des Kryptomaterials (Erzeugen, Nutzen und Zurückziehen bzw. Vernichten von Zertifikaten und Schlüsseln) ist in einem Kryptokonzept zu regeln, dies sollte die gesamte Prozesskette – von der Scorebox bis zur Veröffentlichung von Kfz-Daten für allgemeine Forschungszwecke – umfassen.

Für Hinweise zu konkreten Umsetzungsmaßnahmen, die die Versicherung ohnehin umzusetzen hat, gilt das gleiche, was oben zur „Sicherung der Integrität“ ausgeführt wurde. Hier fehlt es noch an einem spezifischen SDM-Baustein.

Die Sicherung der Vertraulichkeit der Kfz-Daten vor Kenntnisnahme durch die **Kfz-Werkstatt** ist differenziert herzustellen. Auf die Kfz-Daten kann an der OBD2-Schnittstelle, offenbar ohne weitere Hürde nehmen zu müssen, zugegriffen werden. Solange diese Schnittstelle nicht besser technisch geschützt ist, können die zum Einbau lizenzierten Werkstätten nur vertraglich gebunden werden, nämlich, dass die Kfz-Daten, sofern sie nicht der rein technischen Analyse des Kfz-Zustands dienen, nicht eingesehen oder genutzt werden dürfen. (#BRW01, #BRW02) Dass die Werkstatt die Inhalte der Scorebox nicht auslesen und auf eigenen Medien speichern können, muss durch technische Sicherungsmaßnahmen erfolgen, die bereits im vorigen Abschnitt zur Sicherung der Integrität angesprochen wurden. Entscheidend zur Sicherung der Vertraulichkeit gegenüber der Kfz-Werkstatt wäre die sofortige Verschlüsselung der Kfz-Daten und das Abspeichern dieser Daten im verschlüsselten Zustand in der Scorebox.

Die Sicherung der Vertraulichkeit vor dem **Scorebox-Hersteller** und dem **Funknetz-Provider** kann durch Verschlüsselung der Daten während der Speicherung und des Transfers sichergestellt werden. Bei der Verschlüsselung der Daten muss dafür gesorgt werden, dass es die Versicherung ist, die über

die Generierung des Schlüssels bestimmt. Dass die Scorebox eine wirksam integre Verschlüsselungsmethode nutzt, müsste mit Hilfe eines Testverfahrens der Scorebox durch eine unabhängige Instanz (Audit) bestätigt werden. Eine zusätzliche Transport-Verschlüsselung zwischen der Scorebox und dem Cloud-Speicher sollte vorgesehen sein, zumal sie weder bei einem store-and-forward-Modus noch als Webservice einen nennenswerten Aufwand mehr bedeutete. Durch die Verschlüsselung würde eine wesentliche Anforderung zur Vertraulichkeitssicherung auch gegenüber den anderen Auftragnehmern durchgesetzt. ***Diese Maßnahmen wäre die wichtigste Schutzmaßnahme, die relativ kostengünstig eine gute Schutzwirkung für das Verfahren insgesamt entfaltet.*** (#BRV08, #BRF01, #BRW01, #BRC01, #BRVert08, #BRM01)

Der Modellfall sieht die Verwendung einer selbst entwickelten und nicht offen gelegten Verschlüsselungsmethode, für den Transfer der Daten aus der Scorebox zur Cloud vor. Dieser Ansatz entspricht nicht dem Stand der Technik. Die Entwicklung eines sicheren kryptographischen Algorithmus‘ setzt eine spezielle wissenschaftliche, insbesondere mathematische Vorbildung voraus. Vor der praktischen Anwendung sind umfangreiche Untersuchungen auf Schwachstellen erforderlich, die von Einzelnen oder kleinen Gruppen nicht geleistet werden können. Sollte der Algorithmen-Entwickler die Geheimhaltung des Verfahrens als Teil von dessen Sicherheit ansehen, so hätte er dadurch das so genannte Kerckhoffsche Prinzip verletzt.[25] Es sind eine Reihe dem Stand der Technik entsprechenden kryptographischen Algorithmen verfügbar, die keine Kosten aus Schutzrechten für geistiges Eigentum, wie Patente, verursachen. Einmalige Kosten entstehen durch die Implementation der kryptographischen Verfahren, laufende Kosten durch die Pflege der Implementation, und – in viel größerem Maße – durch ein korrektes Handling der dafür notwendigen Zertifikate und Schlüssel, das bei „hohem Schutzbedarf“ unabdingbar ist und in einem Kryptokonzept (siehe „Integritätssicherung“) zu entwickeln wäre.

Die Sicherung der Vertraulichkeit vor dem **Cloud-Betreiber** wäre durch eine Verschlüsselung in der Scorebox erreicht. (#BRC01, #BRVert06)

Die Sicherung der Vertraulichkeit vor unbefugt zugreifenden **Sicherheitsbehörden** wäre durch eine Verschlüsselung der Daten ebenfalls umgesetzt (#BRS01). Sicherheitsbehörden sind gehalten, entweder direkt an der OBD2-Schnittstelle oder auf der Ebene bei der Versicherung auf Daten zuzugreifen. Der rechtlich zweifelsfreieste und operativ leichteste Zugang seitens der Sicherheitsbehörden würde über die Versicherung erfolgen, was eine wesentliche Schutzmaßname zur grundsätzlich bestehenden Möglichkeit der Sicherung der Beweiswert-erhaltenden Integrität, Vertraulichkeit, Nichtverkettung und Intervenierbarkeit darstellt (#BRS01). Verschlüsselt gespeicherte Daten der Scorebox sichern auch vor dem unbefugten Zugriff durch **Cracker (#BRVert08, #BRH01)**.

Als Empfehlungen zur Umsetzung von Vertraulichkeitsanforderungen auf der Ebene einzelner Maßnahmen liegen im Kontext des SDM bislang keine Textentwürfe vor. Deshalb verbleibt bis auf weiteres nur die Empfehlung, entsprechende Sicherungsmaßnahmen dem Maßnahmenkatalog des IT-Grundschutzes unter der Maßgabe zu entnehmen, dass die Schutzwirkung der Maßnahmen dem Betroffenen des Verfahrens zu gelten haben.

[25] Das „Kerckhoffsche Prinzip“ gilt nach dem Stands der Technik als wesentliche Eigenschaft von Verschlüsselungsverfahren. Es verlangt, dass die Sicherheit eines Verfahrens ausschließlich von der Geheimhaltung der Schlüssel, nicht jedoch der Algorithmen abhängen darf.

3.1.5. Sicherung der Transparenz

Wesentliche Maßnahmen zum Erreichen von Transparenz eines Verfahrens sind die *Spezifikation* des Verfahrens mit seinen einzelnen Bestandteilen, die *Dokumentation* der Prozessabläufe, der IT-Systeme und Datenbestände, und die *Protokollierung/Quittierungen* von Ereignissen der IT-Systeme, Administrationsvorgängen und Prozessabläufen sowie der Visualisierung im Kfz, dass es derart vollüberwacht wird. (#BRV03, #BRTrans01, #BRW02, #BRTrans02, #BRM02)

Das Erkennen von Mängeln im Rahmen dieses DSFA-Projekts würde dazu führen, dass entsprechende Anforderungen in einem Pflichtenheft formuliert würden, die der Verantwortliche zu erfüllen hätte. Im vorliegenden Modellfall fehlen bspw. wesentliche Informationen, die entweder durch die Fortsetzung der Arbeit der Projektgruppe zu spezifizieren wären oder die durch eine prüffähige Dokumentation insbesondere der einzelnen Prozesse und der IT der beteiligten Organisationen beizubringen wären.

Durch die Selbstanwendung der Gewährleistungsziele auf die Prozesse der Spezifikation, Dokumentation und Protokollierung sind spezielle Maßnahmen dafür zu treffen, dass auf den Empfängerhorizont zugeschnittene, kontrollierbare (Relevanz), prüffähige (Soll-Ist-Bilanzen) und rechtlich beurteilbare Informationen zum Verfahren die Betroffenen und Kontrollbehörden erreichen (Verfügbarkeit der Transparenz). Die Integrität der Spezifikation, Dokumentation und Protokollierungsdaten, die die verschiedenen Organisationen auf verschiedenen Ebenen zu erzeugen haben, muss gesichert werden. Hierzu können Versionierungen und Signaturen zur Sicherung von Dokumentationsständen beitragen. So sind bei hohem Schutzbedarf Protokolldaten insbesondere dem Zugriff der Administration von Produktionsmaschinen zu entziehen, weshalb das SDM den Betrieb sowohl eines Ticketsystems zum transparentem Beauftragungsprozess sowie eines eigenständigen Protokollservers naheliegt, dessen Zugriffe mit Hilfe eines Rechte- und Berechtigungskonzept geregelt sind und kontrolliert werden.

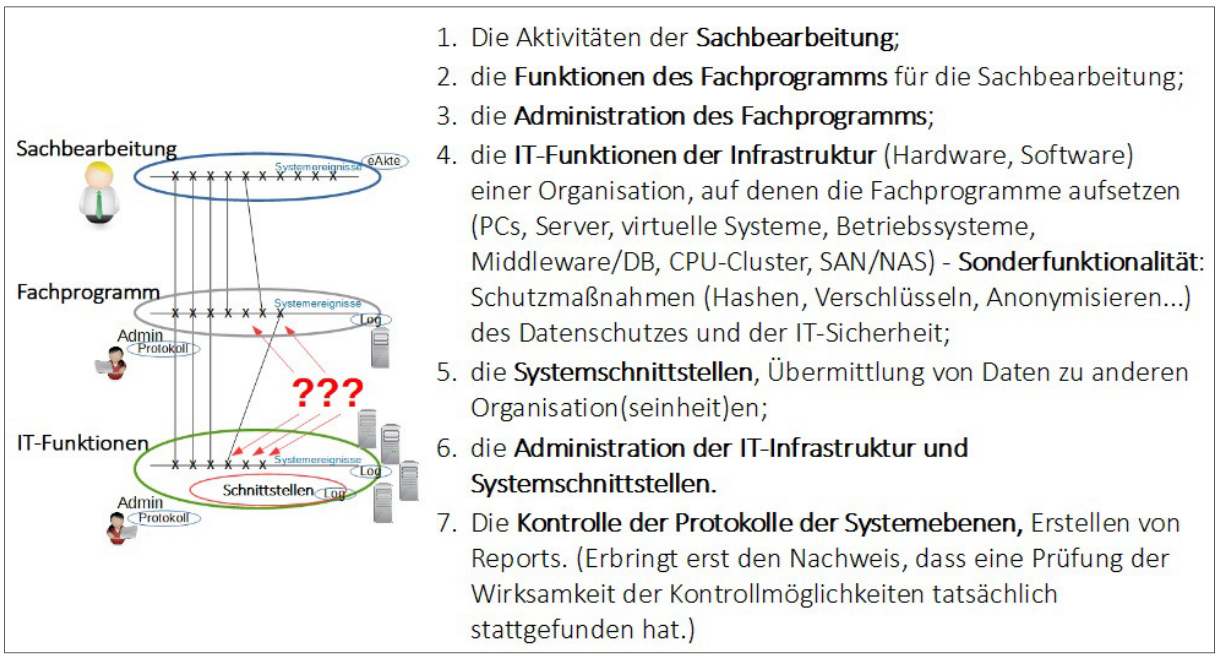


Abbildung 5: Systemebenen, die zu spezifizieren, zu dokumentieren und zu protokollieren sind

Die Sicherung der Transparenz des gesamten Verfahrens, unter Berücksichtigung aller beteiligten Instanzen, ist in der Verantwortung der **Versicherung** (#BRV03). Transparenz ist dabei kein Selbst-

zweck, sondern hat die Funktion, dass die Rechtmäßigkeit des Verfahrens, einschließlich der im Verfahren genutzten Funktionen und Schutzmaßnahmen, auch bei den Auftragnehmern, festgestellt werden kann. Die Dokumentation des Verfahrens versammelt alle relevanten Aspekte, stellt für diese die letztlich rechtlich verankerten Soll-Anforderungen zusammen und zeigt außerdem die Methode auf, mit der die Ist-Zustände der Verfahrenseigenschaften ermittelt und die Prüfergebnisse beurteilt werden können.

Um Prüffähigkeit/Beurteilungsfähigkeit herzustellen muss die Versicherung das Verfahren im Vorhinein spezifizieren (mit Lasten- und Pflichtenheft als konkreten Produkten der Projektphase), sie muss die Komponenten des Verfahrens für den laufenden Betrieb dokumentieren und anhand der Protokollierung in der Lage sein, die Rechtskonformität des Betriebs mit allen seinen Komponenten belegen zu können. Bereits in der Spezifikation des Verfahrens sind die Geschäftsprozesse, Datenbestände, Datenflüsse, sämtliche dafür genutzten IT-Systeme, Betriebsabläufe und Administrationen sowie das Zusammenspiel des Verfahrens mit anderen Verfahren innerhalb und ggfs. außerhalb der Organisation, auf denen das neue Verfahren aufsetzen soll, zu erheben bzw. festzulegen.

Wesentlich ist die Erarbeitung einer vollständigen Konzeption der Prozesse, mit denen die Versicherung den beteiligten Organisationen Anweisungen gibt und die Ausführungen der Anweisungen anschließend nachweisbar kontrolliert. Den Auftragnehmern der Versicherung ist ein Ticketverfahren abzuverlangen, die eine kontrollierte Auftragsannahme und die Prüfung der Ausführung transparent, zweckbestimmt, integer und intervenierbar möglich macht. (#BRInt10)

Bei der Erarbeitung der Komponenten des Verfahrens im Rahmen mehrerer Projektphasen (z.B. Klären des Projektauftrags, Inventarisierung der bestehenden Strukturen, Erarbeiten von Milestones anhand aufeinander aufbauender Teilprojekte) sollten zwischen verschiedenen Phasen Tests durchgeführt und die Tests dokumentiert werden, um permanent Sollvorgaben und Istzustände in der Projektphase aufeinander beziehen zu können. Der hohe Schutzbedarf verlangt, dass die Projektphase nachweislich ihrerseits den Anforderungen der Gewährleistungsziele genügt und auch die Projektphase demnach für alle Stakeholder zumindest innerhalb der Versicherung transparent, zweckbestimmt, interventionsfähig und integer verläuft (durch Dokumentation und Protokollierung von Arbeitssitzungen, Tests von Funktionen und Schutzmaßnahmen sowie Freigaben einer nächsten Projektphase). Zur Erreichung von Transparenz sind in der Projektphase die Verträge mit den externen Auftragnehmern und den Betroffenen zu erarbeiten. (#BRInt10)

Die Versicherung muss die Fallbearbeitung der Sachbearbeitung des Pay-as-you-drive-Verfahrens dokumentieren und protokollieren. Das geschieht typischerweise in Form von (Fall-)Akten, durch die Protokollierung der Programme und der Administrationstätigkeiten und durch die Kontrolle der Protokolle über alle sieben Schichten. Dieser für jedes Verfahren datenschutzrechtlich allgemein gültige Aspekt wird hier nicht weiter ausgeführt.

In diesem Fall ist insbesondere die Berechnung des Scores zu dokumentieren. Es sollte darüber hinaus einer Prüfinstanz auf Verlangen schrittweise das Errechnen eines Scores unmittelbar demonstriert werden können. Hier besteht die Besonderheit, dass es sich um ein Verfahren nach Art. 22 DSGVO handelt. Das bedeutet für die Transparenz, dass die erweiterten Informationspflichten nach Art. 13 Abs. 2 f) und Art. 14 Abs. 2 g) DSGVO neben den üblichen Informationspflichten zu erfüllen sind. Das heißt, dass sowohl für den Betroffenen als auch für staatliche Prüfinstanzen ersichtlich sein muss, welche konkreten Kfz-Daten in die Berechnung des Scores bzw. in die der Beitragshöhe einge-

flossen sind. Dazu muss dem Kfz-Halter nachgewiesen werden können, dass die Daten tatsächlich aus seinem Kfz stammen (Kfz-Authentizität). (#BRInt12)

Der Versicherungsnehmer sollte einmal im Jahr einen Bericht mit den wesentlichen Informationen bezüglich des Pay-as-you-drive-Verfahrens zur Einlösung der Transparenzpflichten aus Art. 5 DSGVO erhalten. In diesem sollte in jedem Fall der errechnete Score mit einer entsprechenden Abstufung der Beitragsgrenzen sowie die Kontaktdaten für einen Ansprechpartner (Single-Point-of-Contact SPOC) und eine Übersicht über Sicherheitsvorfälle innerhalb des Messzeitraums enthalten sein. Dem Kfz-Halter sollte dargelegt werden, dass es sich um eine automatisierte Entscheidungsfindung und Profiling handelt, einschließlich einer Darstellung der Logik, damit er die Tragweite der Auswirkungen des Verfahrens überblicken kann. Zusätzlich enthalten sein sollte eine Erinnerung an die freiwillige Teilnahme und die Möglichkeit zur Beendigung der Teilnahme am Verfahren bzw. Einspruch gegen den errechneten Score (vgl. Art. 13 Abs. 2 f) DSGVO) (#BRTrans06). Gegebenenfalls kann auch ein Einzelverbindungsnachweis enthalten sein, der den Kunden über Funklöcher und Ausfälle der Scorebox in Kenntnis setzt.

Im Kfz sollte gut sichtbar ein Hinweisschild („ACHTUNG: Das Verhalten dieses Fahrzeugs wird zum Zweck der Errechnung des Versicherungsbeitrags für die Insight AG aufgezeichnet.“) angebracht sein, das Fahrer und Mitfahrer über das Tracking des Fahrzeugs in Kenntnis setzt. (#BRM02) Darüber hinaus müssen betroffene Personen die in Art. 13 DSGVO genannten Informationen erhalten.

Die **Kfz-Werkstätten** sollten eine vollständige Protokollierung des Einbaus der Scorebox vornehmen, um der Versicherung die Frage beantworten zu können: Welcher Mitarbeiter hat in welches Kfz in welchem Zeitraum eine (eindeutig identifizierbare) Scorebox eingebaut und zu welchem Zeitpunkt wurde die Scorebox scharf geschaltet? Es sollte nach dem Einbau ein Funktionstest durchgeführt und dokumentiert werden. Die Kfz-Werkstatt sollte im Fahrgastraum das Kfz-Tracking-Hinweisschild anbringen. (#BRW02, #BRTrans01, #BRTrans02, #BRTrans03)

Der **Scorebox-Hersteller** sollte die Scoreboxeigenschaften genau dokumentieren, insbesondere die Eigenschaften der Schutzmaßnahmen, die hier anhand der Gewährleistungsziele aufgelistet sind. Es sollte das Verfahren zum Update der Scorebox und der Konfiguration speziell auf den Versicherungsnehmer dargestellt werden. Ferner sollte ein Testverfahren vorgesehen sein, mit dem die Werkstatt die Funktionalitäten vor dem Einbau prüfen und nachweisen kann. Ein Einzelverbindungsnachweis wäre auf Seiten der Betroffenen wünschenswert, um Probleme beider Verfügbarkeit der Verbindungen nachweisen zu können. Diese können jedoch auch in der Scorebox protokolliert werden. (#BRTrans02, #BRTrans03)

Den **Cloud-Betreibern** ist eine vollständige Dokumentation all derjenigen IT-Systeme und Prozesse und ggfs. der Subunternehmer abzuverlangen, die für das Verfahren zur Zwischenspeicherung von Daten und deren Übermittlung genutzt werden. Dies betrifft insbesondere die Administrationsvorgänge, die im Zusammenhang mit dem Verfahren – gerade auch auf der Ebene der IT-Infrastrukturen einschließlich der Virtualisierung – bestehen. Es sollte ein Ticketsystem genutzt werden.

Wenn **Sicherheitsbehörden** auf die Kfz- bzw. Versicherungsdaten zugegriffen oder wenn es einen **Sicherheitsvorfall** innerhalb der gesamten Prozesskette gab, dann muss der Kfz-Halter im Regelfall darüber unterrichtet werden. (#BRTrans04, #BRTrans05)

Als Empfehlungen zur Umsetzung von Transparenzanforderungen auf der Ebene einzelner Maßnahmen liegen die, im Kontext der Unterarbeitsgruppe „SDM“ erarbeiteten aber noch nicht publizierten, Texte zu „Spezifikation“, „Dokumentation“ und „Protokollierung“ vor.

3.1.6. Sicherung der Nichtverkettung

Die **Versicherung** ist für die gesamte Prozesskette gehalten, auch operativ sicherzustellen, dass die Kfz- und Verhaltensdaten nicht über den festgelegten Zweck hinaus verarbeitet werden (können). Dazu zählt insbesondere das Unterlassen der Weitergabe der Daten. Dafür muss sie, orientiert an der Zweckbestimmung, die Verarbeitung, Nutzung und Übermittlung der Kfz- und Verhaltensdaten für die gesamte Prozesskette auf das unbedingt erforderliche Maß reduzieren und mittels eines Rollen- und Berechtigungskonzept sicherstellen (#BRV06, #BRV08), dass die Fallbearbeitung nur anhand der im Geschäftsverteilungsplan ausgewiesenen, zuständigen Abteilungen und nur nach Durchlaufen eines Authentisierungsverfahrens im Fachprogramm erfolgt. Hierbei ist insbesondere zu berücksichtigen, dass der Forschungsabteilung kein unbeschränkter Zugriff auf die Original-Kundendaten einzuräumen ist. (#BRV05).

Es bedarf eines Forschungskonzepts, in dem als Voraussetzung für einen Zugriff aus Modellierungsgründen die wirkungsvolle Pseudonymisierung/Anonymisierung der Kundendaten zu erarbeiten und festzulegen ist. Die Anonymisierung der Daten durch Löschen oder Ersetzen möglicher Identifikatoren muss in einem Maße umgesetzt werden, das garantiert, dass die Anonymitätsgruppe hinreichend groß und das Risiko einer Deanonymisierung hinreichend klein ist. Die Verwendung von Pseudonymen setzt eine kompetente Unterscheidung von mindestens drei Pseudonymtypen voraus (bspw. Personen-, Rollen-und Transaktionspseudonyme). Dies gilt ebenso für die Weitergabe der Kfz-Daten und der errechneten Verhaltenseigenschaften zu Forschungszwecken. (#BRN02) (#BRN03) (#BRN04)

Es bedarf eines weiteren Konzepts, wie eine Kfz-Weitergabe, etwa durch Leasing oder Verkauf, zu erfolgen hat. Dieses Konzept wäre vermutlich als ein eigenständiges großes Modul im Projekt zu erarbeiten. (#BRN05)

All das ist wirkungsvoll durch ein reifes Datenschutzmanagementsystem zu kontrollieren, zu prüfen und zu beurteilen. (#BRInt03)

Die **Kfz-Werkstätten** sind gehalten, Prozesse zum Auffinden technischer Fehler durch Kfz-Analyse von denen, die in Zusammenhang mit dem Einbau, Umbau, Ausbau, dem Auslesen und möglicherweise auch dem Beschreiben der Scorebox stehen, zu trennen. (#BRW01, #BRW02) Es ist operativ sicherzustellen, dass bei Fehleranalysen keine dafür nicht erforderlichen Kfz-Daten, wie sie für die Score-Berechnung herangezogen werden, erhoben und gespeichert werden. Dies kann weitgehend nur rechtlich sichergestellt werden. Der Kfz-Werkstatt ist darüber hinaus vertraglich zu verbieten, dass die Kfz-Daten an der OBD2-Schnittstelle zu anderen als den vertraglich legitimierten Zwecken im Kontext der Versicherung gelesen, verändert und gespeichert werden. (#BRV07)

Der **Scorebox-Hersteller** kann durch frühzeitige Verschlüsselung der Kfz-Daten in der Box sicherstellen, dass die Daten nicht zu anderen als dem definierten Zweck genutzt werden können, bspw. auch nicht zur unbefugten Geolokalisation (#BRV07). Weil der Hersteller sowohl die Hoheit über die Durchführung der Verschlüsselung als auch über das Funkmodul hat, sind Tests durch unabhängige Instanzen an einer zufällig ausgewählten Scorebox durchzuführen, die überprüfen, ob in der Scorebox nicht nur korrekt (auch vor dem Hersteller der Scorebox) verschlüsselt sondern ob noch weitere Daten gespeichert werden als diejenigen, die von der Versicherung rechtlich gerechtfertigt genutzt

werden und auch ob noch weitere eigenständige Verarbeitungsschritte erfolgen. Etwaiges „Nachhause-Telefonieren“, wie es aktuelle Betriebssysteme vielfach unternehmen, wäre auszuschalten. Die Übermittlung von Berichten aus der Scorebox über ihren technischen Zustand kann abhängig von Werkstattaufenthalten oder anhand der expliziten Freigabe durch den Nutzer erfolgen.

Die **Cloud-Betreiber** und **Funknetz-Provider** sollten nur auf verschlüsselte Daten zugreifen können. Es sollte zusätzlich darauf geachtet werden, dass keine weiteren semantisch zugänglichen Metadaten übermittelt werden, die den Cloud-Betreibern und Funknetz-Providern eine Chance auf Profilierungen eigener Art mit Personenbezug („unique users“) eröffnen (#BRC07).

Außerdem muss durch starke Trennungsmaßnahmen von anderen Verfahren, gerade wenn diese von der gleichen Versicherung betrieben werden, gesichert werden, dass der Cloud-Betreiber nicht Daten unterschiedlicher Kunden bzw. Organisationen verschneiden kann. Auch hier wäre die Datenverschlüsselung in der Scorebox eine ganz wesentliche Schutzmaßnahme. (#BRC02)

Die Sicherung der Nichtverkettung vor unbefugt zugreifenden **Sicherheitsbehörden** und **Cracker** wäre durch eine Verschlüsselung der Daten ebenfalls umgesetzt (#BRV07).

Als Empfehlungen zur Umsetzung von Nichtverkettungsanforderungen auf der Ebene einzelner Maßnahmen liegen die, im Kontext der Unterarbeitsgruppe „SDM“ erarbeiteten, aber noch nicht publizierten, Texte zu „Anonymisierung“, „Pseudonymisierung“, „Trennung“ sowie „Rollen und Berechtigungen“ vor. Ebenfalls von der UAGSDM erarbeitet, aber noch nicht publiziert, ist der Baustein „Datenschutzmanagementsystem“.

3.1.7. Sicherung der Intervenierbarkeit

Die **Versicherung** hat sicherzustellen, dass die Betroffenenrechte im Verfahren wirksam umgesetzt werden (#BRV04). Das betrifft differenzierte Einwilligungs-, Widerruf- sowie Widerspruchsmöglichkeiten durch Implementierung standardisierter Abfrage- und Dialogschnittstellen. Ein Single Point of Contact (SPoC) für Betroffene sollte nicht nur mit Blick auf dieses Verfahren eingerichtet sein. Die im Verfahren verwendete IT muss zudem Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche und Gegendarstellungen vorsehen. Es sollten operative Funktionen zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten vorgesehen sein. (#BRIv01)

Die Versicherung muss ferner Prozesse vorsehen und auf IT-Systeme zugreifen können, mit denen Störungen und Probleme im Verfahrensablauf und bei den Schutzmaßnahmen für Datenschutz und IT-Sicherheit erkannt und bearbeitet werden können („Changemanagement“). (#BRIv02)

Ein Abschalten der Scorebox vor Fahrtbeginn ist konzeptionell nicht vorgesehen. Dies wäre jedoch zumindest dann notwendig, wenn ein Zweitnutzer des Kfz grundsätzlich keine Auswertung seines Fahrverhaltens wünscht. (#BRM03) Denkbar wäre außerdem, dem Kfz-Halter die Option auf durch die Scorebox nicht-beobachtete Fahrten einzuräumen, was in einem kleinen Rahmen und als verteuernde Extra-Versicherungsoption angeboten sinnvoll sein könnte.

Bei hohem Schutzbedarf bedeutet Löschen ein wirksames Entfernen im Sinne des Vernichtens sowie das Erbringen eines Nachweises (Quittierung, Protokolleintrag, Auskunft) darüber (#BRTrans01, #BRTrans02, #BRTrans03). Dies gilt für alle beteiligten Organisationen der Prozesskette, und zwar auch dann, wenn es sich um verschlüsselte Daten handelt. Mit dem Austritt aus einer Versicherung

dürfte im Regelfall das Löschen auch der Daten des Versicherungsnehmers verbunden sein. Dies dürfte mit dem Ausbau oder zumindest der Deaktivierung der Scorebox verbunden sein. Fraglich ist, ob die Scorebox in den Besitz der Versicherung oder des Kfz-Halters übergeht. Sollte die Scorebox im Besitz der Versicherung verbleiben, muss für die Scorebox ein sicheres Löschen aller Daten und Konfigurationen („reset“) nach dem Ausbau der Scorebox vorgesehen sein. (#BRN05)

Die **Kfz-Werkstätten** müssen auf Änderungsanforderungen seitens der Versicherung bzgl. des Einbaus, Umbaus, Ausbaus und insbesondere das Updaten von Scoreboxen angemessen reagieren. (#BRInt03, #BRIv02)

Die **Scoreboxhersteller** müssen die Box so konzipieren, dass diese all den hier aufgelisteten operativen Anforderungen tatsächlich entsprechen kann. Das Zurücksetzen der Boxen auf einen definierten Status, der den Datenschutzanforderungen in der Grundeinstellung („by default“) genügt, muss ab Auslieferung vorgenommen und durch die Werkstätten umsetzbar sein. Das Löschen von Daten ist insbesondere bei Speichertechniken auf Grundlage von SSD-Techniken allerdings sehr anspruchsvoll. Hoher Schutzbedarf verlangt ein Löschen im Sinne des „Vernichtens von Daten“. Die Hersteller müssen in der Lage sein, auf Änderungen der operativen Anforderungen durch die Versicherung, die bspw. auf rechtliche Änderungen reagiert, ihrerseits zu reagieren. Die Schnittstelle für das Einspielen von Updates der Scorebox-Software sollte im Grundsatz vom verschlossenen Gehäuse geschützt sein, oder zumindest die Freischaltung einer extern zugänglichen Schnittstelle, etwa der Funkverbindung zur Nutzung von Updates für die Scorebox, initial nur über einen derart innen liegend geschützten Schalter erfolgen. (#BRInt03, #BRIv02)

Die **Funknetz-Provider** und **Cloud-Betreiber** müssen sicherstellen, dass sie die Daten, die bei ihnen zwischengespeichert werden, zeitnah und vollständig löschen und das Löschen auch nachweisen können. (#BRInt03, #BRIv02)

Zu den Anforderungen der Beachtung der Betroffenenrechte sowie der daraus folgenden funktionalen und sicherheitstechnischen Umsetzungen bei den **Sicherheitsbehörden**, wenn diese auf Betroffenendaten bei der Versicherung zugreifen, muss hier kein Gegenstand der Betrachtung sein.

Als Empfehlungen zur Umsetzung von Nichtverkettungsanforderungen auf der Ebene einzelner Maßnahmen liegen die, im Kontext der Unterarbeitsgruppe „SDM“ erarbeiteten aber noch nicht publizierten, Texte zu „Berichtigung“, „Löschen“ und „Sperren“ vor.

3.2 Dokumentation Bewertungsergebnisse (Restrisikoanalyse)

Wenn die Analyse der Restrisiken nur in Bezug auf die Details des Modellfalls durchgeführt wird, sind die verbliebenen Restrisiken des Verfahrens sehr groß, weil im Modelfall nur wenige Maßnahmen zur Verringerung der operativen Risiken vorgesehen sind. Im Wesentlichen sind im Modellfall zwei Maßnahmen vorgesehen: a) die redundante Nutzung einer zweiten Cloud zur Speicherung der Kfz-Daten, die die Verfügbarkeit der Kfz-Daten für die Versicherung verbessert, aber zugleich das Integritäts- und Vertraulichkeitsrisiko erhöht sowie b) eine Verschlüsselung der von der Scorebox zwischengespeicherten Kfz-Daten.

Beide der im Modellfall dargelegten Sicherungsmaßnahmen reichen in keinem Falle aus: Eine Kopie unverschlüsselter Kfz-Daten in eine zweite Cloud reduziert zwar das Verfügbarkeitsrisiko, aber erhöht, gemessen an den Grundsätzen Art. 5 DSGVO bzw. den Gewährleistungszielen des SDM, alle

anderen Risiken. Eine zweifelhafte Transportverschlüsselung simuliert auf dem Papier eine Maßnahme zur Sicherung der Vertraulichkeit, bedeutet aber in der Praxis das Bereitstellen einer komfortablen Abhörmöglichkeit zumindest für den Hersteller der Toolbox, wenn nicht auch für Funknetz-Provider oder Sicherheitsbehörden sowie natürlich unbeteiligter Dritter, zumal wenn diese von dieser konstruktiven Schwäche erfahren sollten.

Eine Analyse weiterhin bestehender Restrisiken, die auch dann fortbestehen, wenn die hier vorgeschlagenen Schutzmaßnahmen installiert werden, ist in der Kürze der Zeit nicht hinreichend praxisgerecht möglich. Eine Restrisikoanalyse ist durchzuführen und rechtlich zu beurteilen, nachdem die hier empfohlenen Schutzmaßnahmen priorisiert, ausgewählt, spezifiziert und implementiert wären.

Die Hauptrisiken, die diese DSFA identifiziert hat, bestehen in der weiter zunehmenden Differenzierung des Modells auf Seiten der Versicherung, die den Eingriff in die Rechte und Freiheiten noch weiter intensivierte, in der nur unzureichenden Beachtung der Rechte betroffener Dritter und in der mangelhaften Überwachbarkeit bzw. Testung der Scorebox auf Seiten des Herstellers, zumal hier typischerweise die Standardbibliotheken bzgl. Kryptomaßnahmen zum Signieren und Verschlüsseln zum Einsatz kommenden dürften. Ferner wären die Aktivitäten im Kontext von Werkstätten, um an die Kfz-Daten zu gelangen und ggfs. zu manipulieren, genauer zu untersuchen. Das größte sicherheitstechnische Risiko im gesamten Verfahren ist die bislang weitgehend ungeregelte Erzeugung von Kfz-Daten und die offene Zugänglichkeit der OBD2-Schnittstelle.

3.3 Implementierung der Schutzmaßnahmen

Dieser Aspekt kann im Rahmen des Modellfalls nicht simuliert werden. Die Implementation von Schutzmaßnahmen selber ist zudem kein Bestandteil des SDM, sondern eine Aktivität des Verantwortlichen. Gemäß den Anforderungen aus Art. 35 DSGVO und entsprechend des Prozessablaufs zur Durchführung einer DSFA nach DSGVO wäre der Verantwortliche aufgefordert festzulegen, welche der empfohlenen Maßnahmen mit welcher Priorität und mit welcher Qualität implementiert und überwacht werden. Dieses Konzept wäre Bestandteil dieses Kapitels.

Das SDM (Methodik-Handbuch V1.0) weist ein Vorgehensmodell aus, mit dem Maßnahmen wirksam umgesetzt und deren Wirksamkeit kontrolliert werden kann.

3.4 Test und Dokumentation der Wirksamkeit der Schutzmaßnahmen

Dieser Aspekt kann im Rahmen des Modellfalls nicht simuliert werden, da hierzu bekannt sein müsste, welche der vorstehend beschriebenen Maßnahmen in welcher Weise umgesetzt sind. Für den weiteren Ablauf des Modellprojektes hält das SDM jedoch einen methodischen Ansatz bereit. Das SDM geht über die Anforderungen an eine DSFA hinaus, weil damit nicht nur bestehende Defizite ermittelt, sondern gleichzeitig passende Maßnahmenempfehlungen zu deren Beseitigung gewonnen werden können.

Der Abschnitt 10 des SDM-Handbuchs V1.0 „Prüfen und Beraten auf der Grundlage des Standard-Datenschutzmodells“ beschreibt die Anwendung des SDM für Zwecke der Prüfung und Beratung. Dieser Prozess geht von einer strukturierten Analyse der Daten, Prozesse und Systeme aus und endet schließlich in einer Rückmeldung über Verstöße gegen Datenschutzrecht einschließlich möglicherweise fehlender technischer und organisatorischer Maßnahmen.

Dieses Ablaufmodell kann nicht nur durch externe Prüfer und Berater angewandt werden, sondern auch durch interne Personen und Teams im Rahmen von organisationsinternen Prüfungen. Diese Prüfungen beschränken sich nicht notwendig auf bereits etablierte Verfahren, sondern können auch in Designprozessen für neue interne Anwendungen, Produkte und Dienstleistungen durchgeführt werden. Das beschriebene Modell ist zyklisch, im Sinne des Deming-Zyklus, angelegt und fügt sich insofern in etablierte Standards für Informationssicherheitsmanagementsysteme in die Geschäftsprozesse von Unternehmen und Behörden ein.

Es liegt seitens der Unterarbeitsgruppe SDM ein Entwurf zu einem Textbaustein für die Initiierung und den laufenden Betrieb eines Datenschutzmanagementsystems vor.

3.5 Nachweis über die Einhaltung der DSGVO

Dieser Aspekt kann im Rahmen des Modellfalls nicht simuliert werden, weil er von der Durchführung aller vorausgehenden Aktivitäten, insbesondere der Auswahl und Implementation sowie des Betriebs der Maßnahmen abhängig ist, die sich ebenfalls nicht sinnvoll simulieren lassen.

Der Nachweis der Wirksamkeit der hier empfohlenen Schutzmaßnahmen würde ganz überwiegend anhand der Beurteilung von Protokollen durchzuführen sein.

Der Nachweis der Rechtskonformität eines Verfahrens geschieht anhand einer Beurteilung der rechtlichen Regelungen (Gesetzeslage und Verträge) sowie funktionaler Aspekte des Verfahrens, die im Hinblick auf das Erfüllen rechtlicher Anforderungen ausgewählt und konfiguriert wurden. Das SDM unterscheidet zu diesem Zweck a) den Aspekt der Kontrollierbarkeit, der Bezug nimmt auf Beachtung der *Relevanz der aufgeführten Komponenten* für ein Verfahren, b) den Aspekt der Prüfbarkeit, der Bezug nimmt auf die *Erstellung von Prüfergebnissen aus Soll-Ist-Bilanzen für die Komponenten* und c) den Aspekt der *Beurteilbarkeit der Prüfergebnisse* der Soll-Ist-Bilanzen durch Rückbezug wieder auf die rechtlichen Vorgaben. Diese Systematik bietet eine zweckgemäße, transparente und integre Form zum Erbringen dieses geforderten Nachweises der Wirksamkeit der Verfahrensgestaltung und der Schutzmaßnahmen. Die vorliegende DSFA hat versucht, alle relevanten Verfahrenskomponenten und Beteiligte auszuweisen und die Bildung von Prüfergebnissen zu ermöglichen.

4. Berichterstellung

4.1 Erstellen DSFA-Bericht

Der vorliegende Text stellt den geforderten Bericht dar, der sich an den Verantwortlichen als den Hauptempfänger richtet.

In der nachfolgenden Tabelle sind die Risiken, die in Kapitel 2 identifiziert wurden, durch #R*Risikobezeichner* gekennzeichnet. Die dazugehörigen Schutzmaßnahmen zur Minimierung der Risiken, die in Kapitel 3 aufgelistet sind, sind durch #BR*Risikobezeichner* auffindbar (Beispiel: Ausführungen zur Schutzmaßnahme des Transparenzrisikos „#RV03“ sind durch den Textmarker „#BRV03“ auffindbar):

Zusammenstellung von Risiken	Versicherung	Hersteller Scorebox inkl. Funkeinheit	Werkstätten	Funknetz-Provider	Cloud-betreiber 1,2	IT-Sicherheit, Hacking	Sicherheitsbehörden	Mitfahrer
Datenminimierung	#RD01 #RV02	#RHS01 #RD01	#RD01	#RD01	#RD01		#RS01	
Verfügbarkeit	#RVerf01 #RVerf03	#RHS01 #RSB01			#RCVerf03			
Integrität	#RInt01 #RInt02 #RInt03 #RInt10 #RInt11 #Rint12 #Rint13	#RHS01 #RHS02 #RP02 #RInt01 #RInt05	#RW03 #RW04 #RInt01 #RInt04	#RInt01	#RInt01 #RInt06	#RH01 #RInt08 #RInt09	#RS01 #RInt01 #RInt07	
Vertraulichkeit	#RV08 #RVert01 #RVert02 #RVert03	#RHS01 #RP02 #RV08 #RF01 #RVert05	#RW01 #Rvert04	#RP01	#RC01 #RVert06	#RH01 #RVert08	#RS01 #RVert07	#RM01
Transparenz	#RV03 #RTrans01 #RTrans02 #RTrans03 #RTrans04 #RTrans05 #RTrans06	#RTrans01 #RTrans02 #Rtrans03	#RW02 #RTrans01 #RTrans02 #RTrans03	#RTrans02	#RTrans02	#RH01	#RS01 #RTrans02	#RM02
Intervenierbarkeit	#RV04 #RVerf02 #RIv01 #Riv01 #Riv02	#RHS01 #Riv02	#RW04 #Riv02	#RIV02	#Riv02	#RH01 #RIv02	#RS01	
Nichtverkettung	#RV02 #RV05 #RV06 #RV07 #RV08 #RN01 #RN02 #RN03 #RN04 #RN05	#RHS01 #RP04 #RV07 #RF01	#RV07 #RW01 #RW02	#RP01	#RC01 #RC02	#RH01	#RS01	

Tabelle 5: Auflistung der beteiligten Organisationen und Risiken

Das Ergebnis der vorliegenden Untersuchungen nach dem SDM ist eine systematische Zusammenstellung von Datenschutzrisiken und Maßnahmen, mit denen diesen Risiken begegnet werden kann. Diese Maßnahmen sind jedoch noch nicht umgesetzt und ihre Wirksamkeit für den konkreten Anwendungsfall noch nicht bewertet.

Nur wenn die empfohlenen Maßnahmen vollständig umgesetzt sind, kann der produktive Einsatz des Verfahrens datenschutzrechtlich zulässig sein. Die Maßnahmen müssen jedoch in einem Sicherheitskonzept dokumentiert werden und ihre Tauglichkeit muss in der Praxis im Rahmen des Datenschutz- und Informationssicherheitsmanagements nachgewiesen sowie einer weiteren *Restrisikoanalyse* unterzogen werden, die zu einer weiteren Konkretisierung der Maßnahmen oder auch zu weiteren Maßnahmen führen kann. Im Anhang Abschnitt III wird beschrieben, wie das Verfahren aus datenschutzrechtlicher Sicht, durch einen anderen architektonischen Zuschnitt, verbessert werden kann mit dem Ziel der Minimierung der Eingriffsintensität.

4.2 Veröffentlichen DSFA-Bericht (Kurzfassung)

Weil es sich nur um ein Planspiel handelt, kann die Anfertigung eines Kurzberichts entfallen.

4.3 Unabhängige Überprüfung der DSFA-Ergebnisse

Diese Anforderung wird durch den Zuschnitt eines Planspiels erfolgen.

Die nach der Veröffentlichung durch die Autoren aufgefundenen Schwächen der hiermit vorgelegten DSFA werden nicht bearbeitet werden, weil es sich nur um ein Planspiel handelt. Im Fall einer DSFA für ein Verfahren in der Praxis müssten die Ergebnisse der externen Überprüfung auf die Gestaltung der Funktionen und Schutzmaßnahmen Einfluss nehmen.

Verbesserungsvorschläge bzgl. des DSFA-Prozessablaufes und des SDM sind im Anhang „Lessons Learned“ (siehe S. 58) aufgelistet.

Teil C – Anhang

I Das Fall-Beispiel

BEISPIELSFALL FÜR DIE DURCHFÜHRUNG EINER DATENSCHUTZFOLGENABSCHÄTZUNG

Sachverhalt: Kfz-Telematikversicherungstarif mit Erfassung an der OBD Schnittstelle

Die Kfz-Versicherung Insight AG möchte einen Tarif anbieten, bei dem der Versicherte einen Bonus auf seine Prämie erhält, wenn sein Fahrverhalten entsprechend „sicher" ist. Der Tarif soll nur Privatkunden angeboten werden. Ob und wie hoch die Einsparung am Ende eines Versicherungsjahres ist, wird durch einen internen Algorithmus zum Jahresende bestimmt (Score). Die erhobenen Daten werden an einen Cloud-Service übertragen, dessen Firmensitz in Bangladesh ist. Backups sowie Wartung finden über einen weiteren US-Cloud-Service statt – dieser besitzt hierfür einen EU-Standardvertrag. Aus dem Score errechnet die Versicherung dann die monetäre Einsparung. Diese kann im schlechtesten Fall Null sein; eine Erhöhung der eigentlichen Prämie kann durch die Analyse des Fahrverhaltens nicht erfolgen.

Dem Versicherten wird bei Vertragsabschluss in einer Werkstatt ein Gerät in das Kfz einge-baut, das am CAN-Bus des PKWs angeschlossen ist (ODB2 Schnittstelle). Über diesen Bus werden folgende Daten erhoben:

- Fahrgestellnummer
- GPS-Position mit einer Genauigkeit von 1 - 3 Metern
- Höhe
- Beschleunigungswerte
- Uhrzeit
- Motordrehzahl, Drosselklappenstellung, Motortemperatur, Motorlast
- Batteriespannung
- Merkmale des Kfz (Marke, Modell, Baujahr)
- Sitzposition
- Güte der Bremsbeläge
- Servicemeldungen wie z.B. Ölfüllstand, Wartung, Glühlampe defekt

Die Abtastfrequenz eines Datensatzes beträgt eine Sekunde. Im Backend der Versicherung findet ein Mapping der Daten auf die unterschiedlichen Karten mit Geschwindigkeitsbegren-zungen statt. Durch selbstlernende Algorithmen sollen Gegenden, Fahrstrecken und Uhrzei-ten mit einem erhöhten Unfallrisiko ermittelt werden (Big Data). Dazu werden die GPS-Positionen mit allen öffentlich zur Verfügung stehenden Zusatzinformationen angereichert.

Aus den Daten errechnet die Versicherung unter Einbeziehung der obigen Daten und von

- Fahrtroute,
- Geschwindigkeit,
- Verlangsamung/Bremsen vor Abzweigungen/Kreuzungen,
- Beschleunigung nach Abzweigungen/Kreuzungen,
- Bremsen vor Kurven,
- Bremsen auf gerader Strecke,
- Beschleunigung auf gerader Strecke,
- Anzahl der über die App aufgezeichneten gefahrenen Kilometer,
- Anzahl der über die App aufgezeichneten Fahrten,

- Geschwindigkeitsbegrenzungen auf den Fahrtstrecken,
- Straßentypen (Autobahn, Bundes-, Landes- oder Ortsstraße),
- Einwohnerdichte in der Umgebung der Fahrtstrecken,
- Uhrzeit und Wochentag,
- Anzahl Kneipenbesuche,
- Anzahl Straßenrennen mit anderen Telematik-Versicherten,
- vermutetem Geschlecht des Fahrers/der Fahrerin und
- vermuteter ethnischer Herkunft des Fahrers/der Fahrerin

den Score, der Aussagekraft bezüglich der Sicherheit des Fahrverhaltens geben und als Grundlage für die Tarifeinstufung dienen soll.

Die Datenübertragung wird über die mobile SIM-Karte des ODB2-Gerätes an den Cloud-Dienstleister übertragen. Dazu wird ein selbstentwickeltes kryptographisches Verfahren ein-gesetzt, da dieses nach Angabe des Anbieters das höchste Sicherheitsniveau verspricht. Eine Transportverschlüsselung bzw. Inhaltsverschlüsselung mit anerkannten Algorithmen findet nicht statt. Die Daten werden über das interne Netz des Telekommunikationsanbieters sowie ab dem DE-CIX-Knoten in Frankfurt über das Internet übertragen.

Die Rohdaten aus dem Kfz werden 3 Jahre aufbewahrt. Danach werden die GPS-Daten durch Entfernung der Fahrgestellnummer anonymisiert. Die anonymisierten Daten werden zur Weiterentwicklung der Algorithmen und zur Unfallforschung unbegrenzt aufbewahrt und genutzt.

Rechtlich soll der Datenumgang durch einen Vertrag zwischen Versicherung und Kunde ab-gebildet werden. Dieser besitzt eine Textkomplexität nach der Flesch-Methode von 30 Punkten.

II „Lessons Learned“

Es wurden in den letzten Wochen in mehreren Projekten (darunter AppPETs, PARADISE, VVV)[26] sowie anhand des vorliegenden Planspiels Datenschutz-Folgenabschätzungen auf der Grundlage des SDM und des FP-Ablaufmodells durchgeführt, das im Rahmen des Forum Privatheit[27] entwickelt wurde (Bieker et al. 2016). Eine kritische Bestandsaufnahme der dabei gemachten Erfahrungen führte dazu, dass das FP-Modell und das SDM weiter entwickelt werden konnten. Die inzwischen identifizierten Weiterentwicklungsmöglichkeiten wurden für diesen Text jedoch noch nicht genutzt.

a) Es sollte bei dem zu prüfenden Verfahren zumindest in groben Zügen auch die beabsichtigte generische technische Architektur umrissen werden. Eine generische Skizze eines „Techniklayers“ erleichtert es Verfahrensarchitekten, Teilaspekte des Verfahrens zu identifizieren und einzelne Module abzugrenzen, um die Komplexität des Prüfverfahrens zu verringern und Anforderungen insbesondere an die Transparenz, Integrität und Intervenierbarkeit bei der Durchführung der DSFA zu erfüllen.

b) Es sollte grundsätzlich versucht werden, ein Verfahren zu modularisieren, auch dann, wenn keine generische Technikarchitektur in der Verfahrensbeschreibung vorliegt. So zeigte sich in einem der Projekte, dass bspw. das Design der Architektur einer Terminfindung anhand einer Kalenderapplikation ganz anders analysiert und konzipiert werden muss als das Design der Komponente einer Geolokalisation, die ebenfalls Bestandteil des projektierten Verfahrens sein sollte. Im FP-Ablaufmodell sollte ein Splitting des Prüfens ab Block 2.2 vorgesehen werden, so dass die Prüfabläufe zwischen den Blöcken 2.2 und 3.3 (siehe „FP-Modell“ auf S. 5) parallel durchzuführen wären.

c) Es sollte im DSFA-Prozessmodell stärker als bislang die Prozessstruktur entlang des Artikels 35 DSGVO nachvollzogen werden können. Hiernach wären vier große Prozessschritte bei der Durchführung einer DSFA zu unterscheiden:

1. Anhand des Zwecks der gewünschten Funktionalität eines Verfahrens ist anhand der **Relevanzschwelle** zu klären, ob eine vollständige DSFA durchgeführt werden musst. Das bedeutet, dass in jedem Falle für ein personenbezogenes Verfahren dieser erste Schritt einer DSFA durchzuführen ist. Dieser erste Schritt muss deshalb ausgeführt werden, um im Falle eines negativen Ergebnisses, nämlich dass keine vollständige DSFA durchgeführt werden muss, die Begründung dieses Ergebnisses vorlegen zu können.
2. Wenn eine DSFA durchzuführen ist, besteht die wesentliche Aktivität dieses zweiten Prozessschrittes darin, **Normen in funktionale/operative Anforderungen zu transformieren**. Das bedeutet, bestehende normative Anforderungen in das Design der Funktionalität des Verfahrens einfließen zu lassen und dafür operative Anforderungen zu formulieren. Diesen Prozessschritt unterstützt das SDM in besonders intensiver Weise.
3. Die **Überwachung der Umsetzung von Maßnahmen**, die aus den operativen Anforderungen heraus bestimmt wurden, ist der dritte Schritt, der in der Praxis im Rahmen eines Datenschutzmanagements zu leisten ist, das sinnvollerweise alle Verfahren umgreift, nicht nur dasjenige, für das aktuell eine DSFA durchgeführt wird. Auch für die Umsetzung dieses Aspekts sieht das SDM eine spezifisch auf Datenschutzanforderungen abgestimmte Methodik vor.

[26] AppPETs-Projektseite: http://app-pets.org/home/ - PARADISE-Projektseite: http://privacy-paradise.de/ - VVV-Projektseite: https://www.keys4all.de/ - SeDaFa-Projektseite: https://www.sedafa-projekt.de/ .
[27] https://www.forum-privatheit.de

4. Aus den Ergebnissen dieser Überwachung heraus kann es dem Verantwortlichen dann ermöglicht werden, **die Wirksamkeit der Schutzmaßnahmen zu prüfen und nachzuweisen**, wie es Art. 35 DSGVO fordert.

d) Eine DSFA sollte, neben einem expliziten Angreifermodell, auch über ein explizites Vertrauensmodell verfügen. Obwohl es logisch vielleicht nicht nötig wäre, weil das eine aus dem anderen folgen kann, hat es sich zur Kommunikation unter allen beteiligten Professionen als heuristisch nützlich erwiesen darzulegen, wie hoch der Vertrauensbedarf in Techniken, Infrastrukturen, Organisationabläufe, in das korrekte Funktionieren von Institutionen und nicht zuletzt in Personen ist. Dieser Aspekt sollte sowohl im FP-Ablaufmodell („Block 2.2“) als auch im SDM („Risikoanalyse“) Eingang finden.

e) Im Kontext des SDM wäre es hilfreich, den Typ von Schutz zu bezeichnen, der durch ein funktionales Design sowie durch Maßnahmen, die bislang undifferenziert als „Schutzmaßnahmen“ bezeichnet sind, erreicht werden soll.[28] Diese Differenzierung erleichtert es insbesondere den mit der Implementation befassten Technikern, den Auftrag an sie zu klären, weil das Wort „Schutzmaßnahmen“ vielfach einen zu engen Kontext generiert, der allein die Sicherung der Vertraulichkeit und Integrität als Abwehrziele in den Vordergrund stellt. Hiernach würde es sich empfehlen, die im SDM identifizierten Maßnahmen einem der folgenden vier Typen zuzuordnen:

a) **Design-Maßnahmen** – Design-Maßnahmen entfalten Schutz dadurch, dass der funktionale Kernprozess eines Verfahrens bereits so gestaltet ist, dass gar keine weitere Schutzmaßnahme erforderlich ist. Als Beispiel aus dem Planspiel: Die Errechnung des Scores in der Scorebox würde alle Grundrechtsrisiken, die durch die Nutzung von Cloud-Diensten entstehen, obsolet machen. Dies setzt die Anforderung des Datenschutzes durch Technikgestaltung des Artikels 25 Abs. 1 DSGVO um und wäre als Data-Protection-By-Design im engen Sinne zu verstehen.
b) **Ermächtigungsmaßnahmen** – Diese Maßnahmen entfalten Schutz dadurch, dass sie bestimmte Funktionen bereitstellen, die dem Betroffenen indirekt oder direkt nützen. Indirekter Schutz kann bspw. entstehen, wenn durch Maßnahmen der Transparenz auf Seiten der Organisation die Prüfbarkeit der Design-Maßnahmen, der Beschränkungsmaßnahmen und der Kontrollmaßnahmen hergestellt wird. Ein direkter Schutz für den Betroffenen besteht darin, wenn er in die Lage versetzt wird, unmittelbar durch eigene Aktivitäten Schutzfunktionen eines Verfahrens zu nutzen. Ein typisches Beispiel wäre die Möglichkeit zu schaffen, dass der Nutzer Adblocker, Virenschutzmaßnahmen oder Verschlüsselungsprogramme installiert.
c) **Beschränkungsmaßnahmen** – Diese Maßnahmen entfalten Schutz dadurch, dass sie mögliche Aktivitäten einer Organisation oder eines externen Angreifers (Crackers) einschränken. Zu diesen Maßnahmen zählen Verschlüsselungsmaßnahmen und Berechtigungen.
d) **Kontrollmaßnahmen** – Diese Maßnahmen entfalten Schutz, indem sie diese vier Maßnahmentypen prüfbar machen. Als Beispiele wären Hashwertebildung und Hashwertprüfungen bzw. Signaturen zu nennen sowie Maßnahmen der Spezifikation und Dokumentation eines Verfahrens sowie die Protokollierung der Prozesse eines laufenden Verfahrens und die Prüfung dieser Protokollierung, die ihrerseits zu protokollieren ist.

[28] Diese analytisch und für die praktische Umsetzung unmittelbar nützliche Erweiterung der SDM-Modellierung von Maßnahmen wurde im Rahmen des PARADISE-Projekttreffens durch Bud Bruger angeregt. Ein Aufsatz zur Untersuchung dieses Vorschlags ist in Planung.

III Empfehlungen zur Verfahrensgestaltung, um es tatsächlich datenschutzrechtlich operativ wirksam zu gestalten

Die Eingriffsintensität, insbesondere die, die durch die Verarbeitung durch die Versicherung entsteht, sowie die Beeinträchtigung durch latente Unsicherheiten der IT ließen sich dadurch wirksam reduzieren, dass die Berechnungen des Scores eines Kfz-Halters aufgrund der erfassten Kfz-Eigenschaften bereits innerhalb der Scorebox erfolgten – unter Inkaufnahme eines sicherlich gröberen, aber eben von der DSGVO gebotenen datenminimierten Berechnungsmodells. Anschließend würden nicht die einzelnen Kfz-Daten sondern nur der bereits berechnete Score, vielleicht einmal in der Woche, an die Versicherung übermittelt werden und zwar nachdem der Versicherte der Übermittlung explizit zugestimmt hat. Das erhöht zweifellos das betriebswirtschaftliche Risiko für die Versicherung, und damit den Versicherungsbeitrag des Kfz-Halters, erlaubte dem Kfz-Halter jedoch eine Skalierbarkeit der Überwachungsintensität. Ein Vertrag muss insofern keine einfach pauschale Übermittlungseinwilligung für sämtliche Daten zu jeder Zeit von jedem Ort enthalten. Zur Differenzierung von Risikofahrern sollte zur Berechnung des abgestuften Versicherungsbeitrags, trotz auch eines wahrscheinlich nur beschränkten Verschneidenkönnens mit weniger als sekundenaktuellen Kontextinformationen (bspw. mit aktuellem Straßenkartenmaterial), ein solche Scoreberechnung allein vollkommen hinreichend sein.[29] Hierbei ist auch zu berücksichtigen, inwieweit gemäß Art. 25 DSGVO vorhandene Lösungen mit „eingebautem Datenschutz“ zu Einsatz kommen können oder sogar müssen.[30,31]

Aber auch in diesem Fall der Scoreberechnung innerhalb der Scorebox wären eine ganze Reihe an Schutzmaßnahmen zu treffen und deren Wirksamkeit zu kontrollieren, zu prüfen und zu beurteilen, insbesondere bei der Herstellung bzw. Programmierung der Scorebox und dem Auslesen und der Wartung der Scorebox durch die Kfz-Werkstätten.

Neben der alternativen Systemgestaltung von Pay-as-you-drive auf Basis einer Berechnung und Aggregation unmittelbar in der Scorebox könnten geeignete Treuhändermodelle das Risiko einer unerwünschten Verkettung oder weitergehenden missbräuchlichen Nutzung der personenbezogenen Daten reduzieren. Eine einfache – und auch schon von Anbietern praktizierte – Idee besteht darin, dass die (Roh- oder voraggregierte) Daten aus dem Kfz nicht an die Versicherung gegeben werden, sondern ein Treuhänder, der keine Kenntnis von den Versicherungsnehmern hat, auf Basis dieser Daten die notwendigen Berechnungen vornimmt. Die Versicherung erhält dann nur das Berechnungsergebnis. In einer solchen Konstellation muss genau geklärt sein, welche Beteiligten welche (datenschutzrechtliche) Verantwortung wahrnehmen müssen (Auftragsverarbeitung? Gemeinsame Verantwortung?) und welche Auswirkungen dies beispielsweise auf die Vertragsgestaltung unter den Beteiligten, auf die Kontrollpflichten und -möglichkeiten sowie auf die Rechtewahrnehmung durch die betroffenen Personen hat.

Das Treuhändermodell lässt sich variieren, indem ein Pseudonymisierungs-Gateway zwischengeschaltet wird, das im Datenfluss zum Berechnungs-Treuhänder dafür sorgt, dass dieser keine eindeutige und dauerhaft verwendete Identifikationskennung erhält, sondern wechselnde Kennungen er-

[29] Dies entspricht im Grundsatz der Übermittlung aggregierter Verbrauchswerte allenfalls im 15-Minuten-Takt bei Smart-Metern von Wohnhäusern an Energieversorgungsunternehmen.

[30] Siehe auch Troncoso et al.: PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance, IEEE Transactions on Dependable and Secure Computing, Vol. 8, Issue 5, 2011, http://ieeexplore.ieee.org/document/5654510/

31 De Fuentes et al.: Assessment of attribute-based credentials for privacy-preserving road traffice services in smart cities, in: Personal and Ubiquitous Computing Journal, Special Issue on Security and Privacy for Smart Cities, 2017.

hält. Die Ergebnisse des Berechnungs-Treuhänders würden zurück über das Pseudonymisierungs-Gateway an die Versicherung kommuniziert, wo sie wieder dem Versicherungsnehmer zuordenbar gemacht würden. Durch Ende-zu-Ende-Verschlüsselung würde das Pseudonymisierungs-Gateway keinen Zugriff auf die durchgeleiteten Daten erhalten.

Auch bei der Datenminimierung wäre anzusetzen. Die Versicherung ist eigentlich verpflichtet, mit dem kleinstmöglichen Set von Personenattributen die Personenmodelle zur Risikoabschätzung zu berechnen. Das steht jedoch in einem vollständigen Widerspruch zum Anliegen der Versicherung, durch möglichst viele, möglichst trennscharfe Attribute zu einem möglichst zutreffenden Risikomodell für Personen zu gelangen. Neben den technischen oder organisatorischen Beschränkungen, die für das Verfahren Anwendung finden, sollten insofern auch übergreifende gesetzgeberische Optionen bedacht werden (#BRV01), die das Scoring von Versicherungen formbar machten (#BRD01). In diesem Zusammenhang wäre es geboten, die Erhebung bestimmter Datenkategorien von vornherein gesetzlich auszuschließen bspw. den Katalog unzulässiger Diskriminierungen auszuweiten. Auf der Grundlage dieser Einteilungen – und nicht, wie im hier vorliegenden Fall, auf der Grundlage einer perfekten Individualisierung – könnte bei der Versicherung geforscht werden, mit welch geringstmöglichem Set an personenbezogenen Daten, also mit welcher geringstmöglichen Eingriffsintensität, eine legitimierbare Unterscheidung (statt unzulässiger Diskriminierung) der versicherten Kfz-Halter möglich ist. Aus der Erfahrung mit Scoring-Verfahren zeigt sich, dass in der Regel wenige Parameter das Risiko maßgeblich erfassen, andere Parameter nur unmaßgeblich zur Bestimmung beitragen. Datenminimierung hieße, dass grundsätzlich nur diese wenigen Parameter genutzt werden dürften.

IV Nachtrag zum Workshop am 19. Juli 2017 in Nürnberg

Am 19.07.2017 fand im Auftrag der Datenschutzkonferenz und auf Einladung und unter der Leitung des LDA Bayern ein Workshop in Nürnberg statt, auf dem die Methodik der vorliegenden DSFA mit einer anderen Methodik zur Erstellung einer DSFA, die sich an verschiedene ISO-Standards anlehnte, verglichen werden sollte. Beide Methoden wurden auf dem Workshop in 45 Minuten währenden Vorträgen vorgestellt. Ein Vergleich wurde dann jedoch nicht durchgeführt, zumal keine Kriterien für den Vergleich abgestimmt waren.

Die Autoren dieser Ausarbeitung bedauern, dass diese Bilanz bislang nicht gezogen wurde, obwohl dies zu tun sicher die ursprüngliche Absicht der Veranstalter und vor allem Auftrag der Datenschutzkonferenz[32] war. Eine systematisch erarbeitete Kritik würde helfen, auch die vorliegende DSFA weiter zu verbessern.

Die Kritik an dieser Ausarbeitung im Rahmen von Fragen und Diskussionen unter den Workshop-Teilnehmern fokussierte vor allem darauf, dass die „Risikoformel" der DSGVO nicht hinreichend beachtet wurde, wonach das Risiko für einen Schadenseintritt mit Wirkung auf die betroffenen Personen anhand der Eintrittswahrscheinlichkeit und Schwere des Schadens eines Ereignisses zu bestimmen sei.

Die Autoren der vorliegenden DSFA weisen darauf hin, dass für einen Grundrechte-orientierten Ansatz die Bearbeitung allein auf Basis der auf Ereignisse bezogenen Risikoformel nicht hinreichend ist. Das zu bearbeitende Hauptrisiko lässt sich weitaus weniger mit dem Blick auf unmittelbar ereignisbasierte mögliche Schäden bei der betroffenen Personen als vielmehr an den Aktivitäten der Organisation erkennen, die Grundsätze der DS-GVO tatsächlich umzusetzen. Ob aus den Grundsätzen ableitbare funktionale Anforderungen auch tatsächlich seitens der Organisation umgesetzt wurden, lässt sich sehr viel genauer beurteilen, als Vermutungen zu Eintrittswahrscheinlichkeiten und Schadenshöhe anzustellen, die am Ende auch nur eine leichte heuristisch gewonnene Führungen geben, um daraus dann Maßnahmen abzuleiten. Gleichwohl ließe sich im vorliegenden Text die Risikoformel häufiger nutzen, um diesem Kritikpunkt nachträglich Rechnung zu tragen.

Ebenso ist den Autoren mit einer gewissen kritischen Distanz zum Text aufgefallen, dass im Kapitel der Risikobewertung Risiken benannt, aber nicht in jedem Falle hinreichend beurteilt wurden. Auch hätte die Simulation der Rollen trennschärfer erfolgen können; so fließen verschiedene Kommentierungs- und Anmerkungsebenen in den Perspektiven auf den Fall, auf die Rollen, auf die Methodik unaufgelöst ineinander. Dies ist vor allem der beschränkten Zeit geschuldet; eine verfeinerte Darstellung kann hier für weitere Klarheit sorgen.

Die Autoren haben beschlossen, diesen Text im Nachgang des Workshops zunächst nur rein redaktionell zu überarbeiten. Der Text ist als ein Beispiel geeignet, wie eine DSFA durchgeführt werden kann, die vor allem auf der Methodik, den Kriterien und Maßnahmen des Standard-Datenschutzmodells basiert und im Übrigen die Empfehlungen des DSFA-Framework des Forums Privatheit umsetzt. Der Nachweis der Geeignetheit des SDM war zentrales Motiv zur Erarbeitung

[32] Auszug aus dem Protokoll zu TOP 8c der 93. DSK: „ Die Vorsitzende schließt die Aussprache zu diesem TOP und stellt fest, dass die DSK den Vorschlag des LDA Bayern zur Bildung einer AG für die Durchführung des beschriebenen Vergleichsverfahrens aufgreift. LDA Bayern wird dazu abfragen, welche weiteren Datenschutzbehörden noch an einer Mitarbeit interessiert sind."

dieses Textes, und dafür bietet er eine hinreichend konkrete Anschauung. Es handelt sich nur um einen Beispielfall, der aus Gründen des Methodikvergleichs im Auftrag der Datenschutzkonferenz bearbeitet wurde. Der Gegenstand der DSFA, nämlich das "pay-as-you-drive-Verfahren", war rein fiktiv gewählt und gezielt um einige datenschutzrechtlich brisante Eigenschaften angereichert. Die vorliegende DSFA ist nicht geeignet, um ein real vorliegendes „pay-as-you-drive-Verfahren“ zu beurteilen. Handelte es sich nicht nur um eine DSFA für die exemplarische Bearbeitung eines fiktiven Modellfalls, sondern um eine DSFA für ein konkretes, in der Praxis eingesetztes Verfahren, wäre eine Nachbearbeitung zwingend erforderlich.

Das im Text herangezogene DSFA-Framework des Forums Privatheit wurde inzwischen, auch aufgrund der Erfahrung mit der Anwendung dieses Usecase, weiter entwickelt. Nach Auskunft der Autoren des DSFA-Frameworks ist die Veröffentlichung der neuen Version des Frameworks für Ende November 2017 vorgesehen. Diese neue Version wird in ihrem Kernbereich weiterhin auf die Methodik des SDM zurückgreifen, einige Prüfschritte wurden jedoch neu orchestriert. Das neue DSFA-Framework wird weiterhin kostenlos zur Verfügung gestellt werden unter:

https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php

Im Ergebnis erscheint den Autoren das folgende Fazit für die vorliegende Untersuchung gerechtfertigt:

Das Standard-Datenschutzmodell ist geeignet, um eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO maßgeblich zu unterstützen. Die Anwendung der 7 Gewährleistungsziele des SDM bietet eine vollständige Betrachtung und Bewertung aller Beeinträchtigungen und Risiken für die Rechte und Freiheiten für die betroffenen Personen, die von der jeweiligen Datenverarbeitung ausgehen. Die Anwendung des SDM bei der Erstellung einer DSFA ermöglichst es somit dem Verantwortlichen, die in Art. 35 Abs. 1 DS-GVO geforderte Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge vollständig vorzunehmen. Zurzeit steht Verantwortlichen bei der Auswahl der geeigneten Maßnahmen lediglich der „Katalog der generischen Maßnahmen zur Umsetzung der Gewährleistungsziele“ aus Kapitel 7 des SDM zur Verfügung. Mit der sukzessiven Veröffentlichung der Bausteine des Maßnahmenkatalogs des SDM wird Verantwortlichen künftig ein wesentlich umfassenderes und sehr komfortabel nutzbares Portfolio an Einzelmaßnahmen zur Verfügung stehen, das die Anwendung des SDM weiter vereinfacht.