Bayerisches Landesamt für
Datenschutzaufsicht

Musterbeispiel „Insight AG – Kfz-Telematik-Versicherungstarif“

Durchführung einer Datenschutz-Folgen-abschätzung nach Art. 35 DS-GVO in Anlehnung an die ISO/IEC 29134

Version 1.0 – Stand: 19.07.2017

Dieses Dokument beinhaltet eine Beschreibung zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA; Englisch: Data Protection Impact Assessment - DPIA) gemäß Art. 35 DS-GVO für ein ausgewähltes Musterbeispiel, das im Rahmen eines gemeinsamen Workshops der Datenschutzaufsichtsbehörden mit verschiedenen Methoden behandelt und diskutiert werden soll. Es sind insbesondere auch die Elemente enthalten, die für einen DSFA-Bericht nach Art. 35 Abs. 7 DS-GVO erforderlich sein können. Das Dokument ist dennoch nicht als vollständiges Werk zu betrachten, sondern als exemplarischer Ansatz, wie eine konkrete Umsetzung in Anlehnung an den Standard ISO/IEC 29134 „Privacy Impact Assessment“ erfolgen könnte. **Die Anforderungen der DS-GVO werden dabei vorrangig behandelt.**

Inhalt

1 Sachverhalt

Die Kfz-Versicherung Insight AG möchte einen neuen Tarif „Telematik 100“ 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 den Cloud-Service „Bengali LTD“ übertragen, dessen Firmensitz in Bangladesch ist. Backups sowie Wartung finden über den US-Cloud-Service „Safeguard Corp.“ statt – dieser besitzt hierfür einen EU-Standardvertrag. Aus dem Score-Wert errechnet die Versicherung dann die monetäre Einsparung. Im schlechtesten Fall gibt es keine Einsparung; 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 eingebaut, das am CAN-Bus des PKWs angeschlossen ist (OBD2-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 sowie 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 Geschwindigkeitsbegrenzungen statt. Durch selbstlernende Algorithmen sollen Gegenden, Fahrstrecken und Uhrzeiten mit einem erhöhten Unfallrisiko ermittelt werden (Big Data). Dazu werden die GPS-Positionen mit allen öffentlich zur Verfügung stehenden Zusatzinformationen angereichert.

Die Versicherung errechnet 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-, Land- 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-Wert, der Aussagekraft bezüglich der Sicherheit des Fahrverhaltens geben und als Grundlage für die Tarifeinstufung dienen soll.

Die Daten werden über die mobile SIM-Karte des OBD2-Gerätes an den Cloud-Dienstleister übertragen. Dazu wird ein selbstentwickeltes, kryptographisches Verfahren eingesetzt, 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 drei 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.

2 Schwellwertanalyse

Zunächst ist zu ermitteln, ob die Durchführung einer DSFA notwendig ist. Dieses Verfahren kann auch „Schwellwertanalyse" genannt werden (eng. „threshold analysis").

Eine DSFA ist gemäß Art. 35 DS-GVO in folgenden drei Fällen durchzuführen:

1. Die Form der Verarbeitung, insbesondere die Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung hat voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge (Art. 35 Abs. 1 DS-GVO).
2. Die Verarbeitung fällt unter eines der Regelbeispiele aus Art. 35 Abs. 3 DS-GVO. Hierzu zählen:
   a) Die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
   b) Die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO.
   c) Die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
3. Die Verarbeitung befindet sich auf einer Liste nach Art. 35 Abs. 4 DS-GVO

Nach den Ausführungen der Einleitung sind im vorliegenden Fall mehrere der genannten Tatbestände betroffen:

- Zum einen sollen neue Technologien zur Analyse zum Einsatz kommen: Neben dem Einsatz eines OBD2-Gerätes zur Datenerhebung sollen selbstlernende, noch nicht fertige Algorithmen zu einer Beurteilung herangezogen werden (Art. 35 Abs. 1 DS-GVO erfüllt).
- Weiterhin wird ein großer Umfang an Daten verarbeitet; dies betrifft mindestens die Abtastfrequenz von einer Sekunde bei einer jeden Fahrt, wenn nicht sogar die Zahl der jeweils genannten Daten (Art. 35 Abs. 1 DS-GVO erfüllt)
- In die Analyse soll auch die vermutete ethnische Herkunft des Fahrers einbezogen werden, was unter die besonderen Kategorien personenbezogener Daten fällt. Hier könnte es sich auch um eine Verarbeitung in hohem Umfang handeln, je nachdem wie viele Fahrer am Ende diesen Tarif nutzen werden (Art. 35 Abs. 3 lit. a DS-GVO erfüllt).

- Zusätzlich erlaubt die Erfassung einer jeden Fahrt umfassende Rückschlüsse über die Lebensweise des Fahrzeughalters, bspw. wie oft das Auto genutzt wird, wie die Freizeitgestaltung aussieht, wo/was und wann gearbeitet wird, wann und wie oft Kneipenbesuche stattfinden, welche Ärzte aufgesucht werden (Art. 35 Abs. 3 lit. a DS-GVO erfüllt).
- Mit der Verarbeitung soll außerdem eine automatisierte Bewertung des Risikos für den Versicherer durch das analysierte Fahrverhalten des Fahrers erfolgen, was wiederum automatisiert zu einer Entscheidung über einen Rabatt und damit zu einer Entscheidung mit Rechtswirkung für die betroffene Person führt (Art. 35 Abs. 3 lit. a, Art 22, Art. 4 Nr. 4 DS-GVO). Durch das Auslesen der Kfz-Daten soll das Risiko eines künftigen Versicherungsfalls ermittelt werden. Dazu werden aus den Daten Rückschlüsse über die Zuverlässigkeit, das Verhalten und den Aufenthaltsort des Fahrzeugführers gezogen. Dies fällt unter die Definition von Profiling nach Art. 4 Nr. 4 DS-GVO. Das Ergebnis soll unmittelbar Auswirkung auf den Anspruch des Versicherten auf einen Rabatt auf seinen Versicherungsbeitrag haben.

Aus der Zusammenschau all dieser Umstände wird abgeschätzt, dass wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen bei folgendem Sachverhalt erkennbar ist:
Es werden Daten erhoben, bei denen es sehr unplausibel erscheint, dass diese unproblematisch für einen Score-Wert verwendet werden können (z.B. ethnische Herkunft). Die ***Eintrittswahrscheinlichkeit*** *und der* ***Schaden*** *der Rechte und Freiheiten würde in diesem Fall ein* ***hohes Risiko*** *für die Betroffenen bedeuten.*

In den "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (WP 248, Stand 04.04.2017) wird folgende Heuristik zur Schwellwertanalyse vorgeschlagen:

Punkt aus "Zehnerregel"	Vorhanden
Scoring	x
Automatisierte Einzelentscheidung (mit Rechtswirkung)	x
Systematisches Beobachten	x
Sensitive Daten	x
Umfangreiche Datenverarbeitung	x
Verkettung von Daten	
Besonders schutzwürdige Betroffene	
Neue Technologien/Verarbeitungen	x
Verarbeitung außerhalb EWR	x
Hürde für den Betroffenen, ein Recht auszuüben bzw. einen Dienst nutzen zu können	

Da 7 von 10 Kriterien erfüllt sind, ist nach WP 248 im Sinne einer „Daumenregel" eine Datenschutzfolgenabschätzung durchzuführen.

Ein Ausschluss der Notwendigkeit der DSFA ergibt sich auch nicht aus einer Liste einer Aufsichtsbehörde (Art. 35 Abs. 5) oder aufgrund einer vorgezogenen DSFA des Gesetzgebers (Art. 35 Abs. 10 DS-GVO)

Ergebnis:
Es ist eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO für diesen Beispielsfall **durchzuführen**.

3 Vorbereitung

3.1 Zusammenstellung des DSFA-Teams

Im Rahmen der Vorbereitung der DSFA sind die zuständigen Personen zu ermitteln, die die DSFA durchführen sollen. Das DSFA-Team besteht im konkreten Fall aus einem interdisziplinären Team, das Kompetenzen u. a. in den Bereichen Datenschutz, Risikoermittlung, Prozessmanagement und in den Fachprozessen mitbringt:

Name	Position	Rolle
Herr Schröder	Geschäftsführer, Insight AG	Der Geschäftsführer Herr Schröder, der auch der Auftraggeber der DSFA ist, behält den Überblick über die Durchführung und übernimmt wichtige Lenkungs- und Entscheidungsfunktionen, insbesondere in kritischen oder unklaren Situationen.
Herr Stromberg	Prozessverantwortlicher (Process owner), Insight AG	Herr Stromberg leitet das DSFA-Projekt und hat die finanziellen, zeitlichen und personellen Aspekte im Blick. Er fügt alle Ergebnisse der Prozessschritte zusammen und berichtet direkt an Herrn Schröder.
Herr Schutz	Datenschutzbeauftragter, Insight AG	Der Datenschutzbeauftragter Herr Schutz übernimmt eine beratende Funktion, vor allem im Hinblick auf die Einhaltung des geltenden Datenschutzgesetzes. Er informiert über die notwendigen Informationen, die ein DSFA-Bericht enthalten muss und identifiziert die betroffenen Datenkategorien.
Frau Asci	IT-Leiterin, Insight AG	Die IT-Leiterin Frau Asci ist die Teilprojektleiterin des technischen Bereiches (Risikobeurteilung nach ISO-Norm, Systemarchitektur usw.).
Frau Recht	Juristin, Insight AG	Die Juristin Frau Recht ist die zweite Teilprojektleiterin und ist für die rechtliche Bewertung der DSFA-Durchführung und Dokumentation zuständig.

Name	Position	Rolle
Herr Kutrapali	Geschäftsführer, Bengali LTD	Herr Kutrapali ist der Geschäftsführer des Cloud Dienstleisters „Bengali LTD“ und steht in engem Kontakt mit Frau Asci und Herrn Stromberg und beantwortet alle Fragestellungen z. B. zum Aufbau der IT-Infrastruktur des Unternehmens oder seinem US-Backup-Dienstleister.

Tabelle 1: DSFA-Team

3.2 Prüfplanung

In der Vorbereitung auf die DSFA ist ein Plan für die Projektdurchführung zu erstellen. Beim zugrundeliegenden Musterfall wird mit dem Managementwerkzeug „Jira“ ein neues Projekt im Unternehmen aufgesetzt. Außerdem werden Meilensteine, Aufgaben und Unteraufgaben definiert. Die definierten Aufgabenpakete durchlaufen bis zu ihrer Fertigstellung mehrere Statusbereiche im Lebenszyklus des Projektes. Vor der Durchführung werden vom Geschäftsführer die Verantwortlichen ernannt und die Rahmenbedingungen und Zuständigkeiten geklärt. Dem Geschäftsführer ist bewusst, dass eine DSFA kein einmaliger Vorgang ist, sondern gerade bei wesentlichen Änderungen am Verfahren oder dem Einsatz von neuen Technologien erneut durchzuführen ist, sodass vielmehr von einem Prozess zu sprechen ist. Dieses Dokument soll die Elemente des ersten DSFA-Berichts, Version 1.0 vom 19.07.2017, beinhalten. Eine erneute Risikobetrachtung soll in regelmäßigen Zyklen stattfinden. Geplant ist hierbei ein Zeitintervall von ca. 12 Monaten.

3.3 Festlegung des Beurteilungsumfangs (Scope)

Die in dieser DSFA betrachteten Verarbeitungsvorgänge des neuen Kfz-Telematik-Versicherungstarifs werden nachfolgend mit allen Datenflüssen beschrieben. Es folgt daher eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen nach Art. 35 Abs. 7 lit. a.

3.3.1 Systemarchitektur

Für die technische Umsetzung des Telematik-Versicherungstarifs „Telematik 100“ wurde durch die Insight AG eine besonders flexible und robuste Systemarchitektur konzipiert, die die grundlegenden Aspekte von Datenschutz und Datensicherheit berücksichtigt. Die Insight AG hat sich hierbei für ein System bestehend aus wenigen zentralen Komponenten mit vier unterschiedlichen Akteuren entschieden.

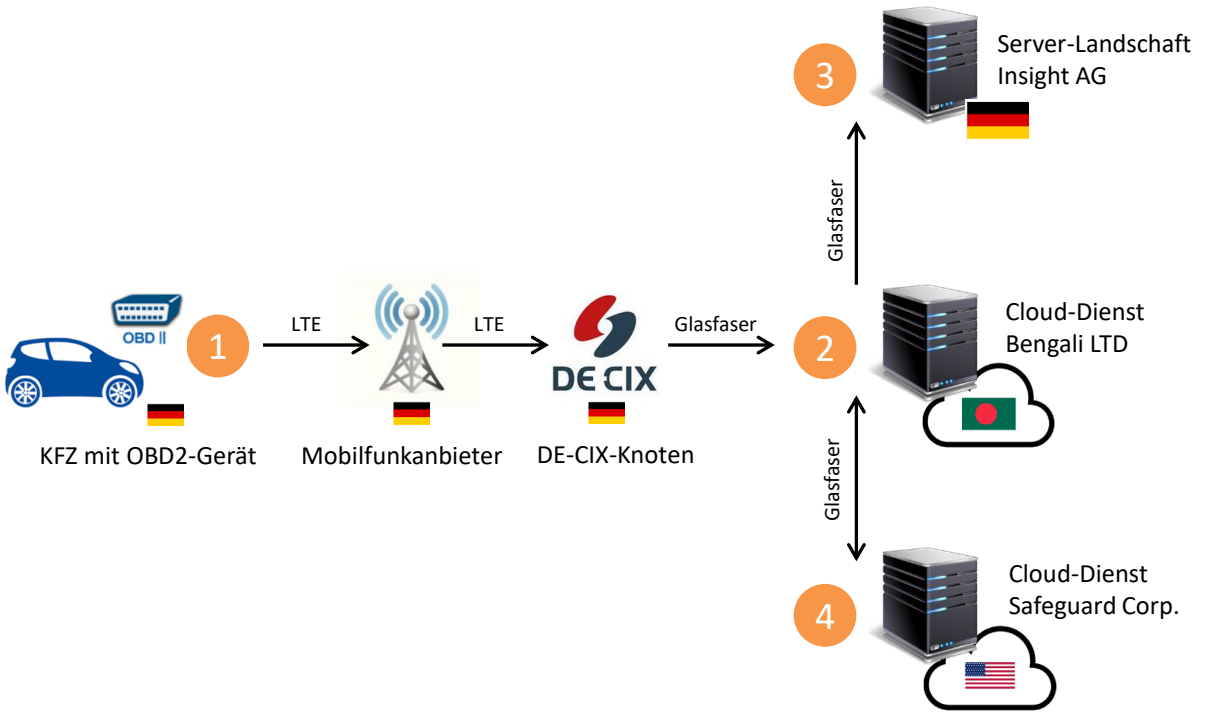


Abbildung 1: Systemarchitektur

Die erste Komponente der Architektur (siehe oben stehende Grafik) befindet sich auf der Seite des Kfz-Versicherten und ist ein durch die Insight AG bereitgestelltes OBD2-Gerät. Durch dieses wird die Datenerhebung für den neuen Tarif erst ermöglicht. Das Gerät wird mit dem Controller Area Network des Fahrzeugs verbunden und sammelt mit einer Abtastrate von einer Sekunde folgende „Fahrzeugdaten":

- 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 zweite essentielle Komponente stellt die Infrastruktur der Bengali LTD dar. Die Rohdaten des Fahrzeugs werden von der Bengali LTD verschlüsselt in einer eigenen Datenbank abgelegt. Diese Rohdaten können dann durch einen entsprechenden Dienst der Insight AG über eine API der Bengali LTD abgerufen werden.

Die dritte Komponente stellt das eigene System der Insight AG dar. In diesem System werden die Rohdaten entschlüsselt, in einem Hadoop-Stack abgelegt und verarbeitet. Die so gespeicherten

Fahrzeugdaten werden durch verschiedene Mappingverfahren qualitativ angereichert. Durch einen internen, selbstlernenden Algorithmus können so folgende „Bewegungsdaten" berechnet werden:

- 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
- Straßentyp
- Einwohnerdichte in der Umgebung der Fahrtstrecken
- Uhrzeit und Wochentag
- Anzahl der Kneipenbesuche
- Anzahl der Straßenrennen mit anderen Telematik-Versicherten
- Vermutetes Geschlecht des Fahrers/der Fahrerin
- Vermutete ethnische Herkunft des Fahrers/der Fahrerin

Der anschließend ermittelte Score-Wert dient der Bonusberechnung für den Versicherungstarif „Telematik 100". Der berechnete Bonus kann jederzeit anhand eines Identifiers einer versicherten Person zugeordnet werden.

Die vierte und letzte Komponente der Systemarchitektur stellt der US-Cloud-Service „Safeguard Corp." dar. Backup und Wartung der Rohdaten des Dienstleisters Bengali LTD wird durch diesen Unterauftragnehmer durchgeführt. Hier werden tägliche Backuproutinen für die Erstellung inkrementeller Backups ausgeführt, die auf Disk- bzw. Flashstorage liegen. Zusätzlich wird wöchentlich eine Vollsicherung der gesamten Rohdaten vorgenommen. Das vertraglich vereinbarte Recovery Time Objective beträgt eine Stunde, wobei das Recovery Point Objective bei maximal 24 Stunden liegt. Sicherungen, die älter als ein Monat sind, werden auf Bandspeicher gesichert. Sobald die Daten auf Band übertragen wurden, werden sie von den anderen Medien entfernt. Die Wartung wird von Mitarbeitern der Safeguard Corp. über Secure Shell durchgeführt. Alle Wartungszugriffe werden umfassend protokolliert.

Nachfolgend werden noch unterstützende Komponenten, sog. „Supporting Assets", aufgeführt:

Typ	Bezeichnung
Hardware	Datenbankserver
	Applikationsserver
	Webserver
	Load Balancer
	Network Attached Storage (NAS)

	Bridge
	Switch
	Gateway
	Firewall
	Router
Anwendungen	Management Information System
	Customer Relationship Management System
	Telematik Application
	Master Data Management System
Datenbanken	Versicherten-DB
	Telematik-DB
	Abrechnungs-DB
Software Umgebung	Windows 10 Enterprise
	CentOS 7
	PostgreSQL 9.6.3
	Apache Tomcat 8.5.16
	Java 8
	Apache Hadoop 2.7.3

Tabelle 2: Supporting Assets

3.3.2 Datenflüsse

Im nachfolgenden Bereich wird dargestellt, an welchen Stellen im Prozess und durch welchen Akteur personenbezogene Daten verarbeitet und übertragen werden. Hierzu wird ein stark vereinfachtes Datenflussdiagramm verwendet:

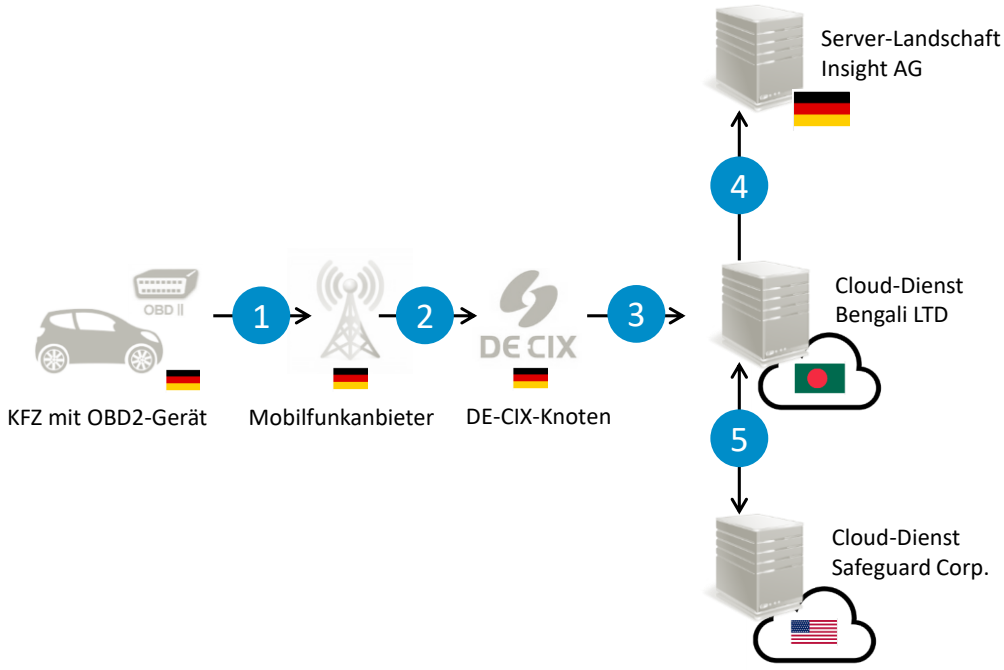


Abbildung 2: Datenflüsse

Im vorliegenden Fall existieren Datenflüsse, die sowohl innerhalb als auch außerhalb der verantwortlichen Insight AG stattfinden. Die initiale Erhebung der Daten erfolgt über ein Gerät, das im Fahrzeug des Versicherten an der OBD2-Schnittstelle installiert wird. Die dort erhobenen Daten

(siehe Nr. 1 in obiger Grafik) werden via LTE (SIM-Karte) über den DE-CIX-Knoten (Nr. 2) in Frankfurt an den Cloud-Dienstleister mit Sitz in Bangladesch (Südasien) (Nr. 3) übertragen. Die Sicherheit der Daten bei einer Übertragung wird durch das von der Bengali LTD entwickelte kryptografische Verfahren „kryptonite" sichergestellt, das von der Insight AG selbst in einem strengen Auswahlverfahren als sicherste Lösung eingestuft wurde.

In Bangladesch werden die Daten verarbeitet und an die Kfz-Versicherung (Nr. 4) zum Errechnen des Score-Werts übermittelt. Der errechnete Score-Wert wird entsprechend dem Versicherten in der Datenbank der Kfz-Versicherung zugeordnet.

Des Weiteren fließen die erhobenen Rohdaten vom Cloud-Dienstleister in Bangladesch zu Backup- und Wartungszwecke an den Dienstleister Safeguard Corp. in den USA (Nr. 5).

3.4 Identifikation und Einbindung von Akteuren und betroffenen Personen

Aus einem Teil der Stakeholder ergeben sich die Akteure und die betroffenen Personen. Diese werden im nächsten Schritt identifiziert und für die DSFA berücksichtigt. Wichtig für die DSFA sind dabei vor allem die folgenden Personengruppen:

- Verantwortliche: Insight AG
- Auftragsverarbeiter: Bengali LTD, Dienstleister Bangladesch
  Safeguard Corp., Dienstleister USA (Subunternehmer)
- Betroffene: Versicherte Privatpersonen
- Weitere Betroffene: Anderweitige Fahrer des Kfz mit eingebauten Gerät

Verantwortlich für den gesamten Prozess der Einführung des Telematik-Versicherungstarifs ist die Insight AG, zu der neben der Geschäftsführung Mitarbeiter aus verschieden Bereichen (z. B. IT-Abteilung, Kundenbetreuung, Marketing) gehören.

Die Insight AG wiederum hat die zentrale Datenverarbeitung nach Bangladesch über ein Auftragsverarbeitungsverhältnis ausgelagert und hierfür den Cloud-Service der Bengali LTD beauftragt. Das Backup und die Wartung der dort anfallenden Datenmengen übernimmt ein weiterer Cloud-Service, die in den USA ansässige Safeguard Corp. Dieser Cloud-Dienst ist nur an die Schnittstelle der Bengali LTD angebunden, nicht jedoch an die Insight AG. Bei diesen beiden Unternehmen spielen für die DSFA ebenfalls die Geschäftsleitung und Mitarbeiter aus bestimmten Bereichen, vor allem aus der IT-Abteilung, eine Rolle.

Neben den beteiligten Unternehmen sind für die DSFA außerdem die Betroffenen selbst, also die Versicherten des Telematik-Versicherungstarifs der Insight AG und sowie weitere Betroffene, wie beispielsweise andere Fahrer des Kfz, wichtig.

3.5 Rechtsgrundlagen

Nachfolgend werden die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert.

Die Vorgänge lassen sich grob dadurch unterteilen, dass die Versicherung einerseits die Daten erfasst (a), eine automatisierte Analyse durchführt, die zu einer Entscheidung über den etwaigen Rabatt führt (b), und außerdem Dienstleister einsetzt, die ihren Sitz in Drittländern haben (c):

a) **Erfassen der Daten bei der Versicherung**
   Grundlage für das Erfassen der Daten bei der Versicherung soll ein Vertrag sein. Dieser kann nach Art. 6 Abs. 1 lit. b DS-GVO als Rechtsgrundlage für die Datenverarbeitung herangezogen werden. Seine Grenze findet dies jedoch in der Erforderlichkeit für die Vertragserfüllung. Es ist bei der Ausgestaltung des Vertrages ebenfalls der allgemeine Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) zu beachten. Hier kann es bei einzelnen Daten fraglich sein, ob diese für die Vertragserfüllung als solches erforderlich sind. Folgende Daten sind hinsichtlich der Erforderlichkeit einer genaueren Prüfung zu unterziehen:
   - Drosselklappenstellung
   - Sitzposition
   - Güte der Bremsbeläge
   - vermutetes Geschlecht
   - Kneipenbesuche
   - ethnische Herkunft

   Als weiterer Grundsatz ist der Grundsatz der Richtigkeit zu beachten (Art. 5 Abs. 1 lit. d DS-GVO). Sofern nur mit vermuteten Daten gearbeitet wird, stellt sich die Frage, ob dies zulässig ist.

   Der Vertrag ist relativ komplex (Index nach der Flesch-Methode 30). Hierbei ist fraglich, ob der Text noch so verständlich ist, dass er einerseits dem datenschutzrechtlichen Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a DS-GVO) und der AGB-Kontrolle nach §§ 305 ff BGB standhält.

   Sofern auch besondere Kategorien von Daten verarbeitet werden, kann ein Versicherungsvertrag nach den Regelungen des Art. 9 DS-GVO nicht als Rechtsgrundlage herangezogen werden. Ein Vertrag allgemein ist ebenso wenig wie der spezielle Versicherungsvertrag in Art. 9 DS-GVO als Rechtsgrundlage vorgesehen. Auch Art. 9 Abs. lit. f DS-GVO, die Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen, kommt nicht in Betracht. Die Vertragserfüllung ist allein schon vom Wortlaut etwas anderes. Es ist weiterhin davon auszugehen, dass die Formulierung bewusst im Vergleich zu Art. 6 Abs. 1 lit. b DS-GVO enger gewählt wurde.

Die vermutete ethnische Herkunft fällt unter die besonderen Kategorien personenbezogener Daten und kann damit nicht auf Grundlage des Vertrages verarbeitet werden. Ggf. könnte die Verarbeitung auf die ausdrückliche Einwilligung gestützt werden (Art. 9 Abs. 2 lit. a DS-GVO). Fraglich ist, ob weitere besondere Kategorien von Daten verarbeitet werden. Es könnte Ausnahmefälle geben, in denen der Versicherungsnehmer bspw. einen Ort anfährt in dessen Umkreis von 1-3 Metern lediglich bestimmte Arztpraxen sind, oder eine Kneipe in der regelmäßig Parteistammtische stattfinden. Hier stellt sich die Frage, ob dies dazu führt, dass Rückschlüsse auf weitere besondere Kategorien personenbezogener Daten ermöglicht werden und damit insgesamt auch die Voraussetzungen des Art. 9 DS-GVO erfüllt werden müssen.

Bei dem Datum Anzahl der Straßenrennen sowie besonders hohen Geschwindigkeitsübertretungen könnte ggf. auch eine Verarbeitung personenbezogener Daten erfolgen, die auf eine strafrechtlich relevante Handlung schließen lässt. Hier ist fraglich, ob auch Art. 10 DS-GVO zu beachten ist. Nachdem aber keine Wertung erfolgt, ob eine Straftat vorliegt, ist der Anwendungsbereich noch nicht eröffnet.

b) Analyse der Daten bei der Versicherung und Festlegen des Tarifs

Rechtsgrundlage für die Analyse der Daten und das Festlegen des Rabattes ist wiederum der Vertrag des Versicherungsnehmers mit der Versicherung. Dazu siehe oben.

Daneben muss Art. 22 DS-GVO beachtet werden.

Die vorliegend geplante Datenanalyse zum Zweck der Anpassung eines Versicherungstarifs ist als Profiling zu bewerten (automatisierte Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte, die rechtliche Wirkung für die betroffene Person entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, vgl. ErwGr 71 DS-GVO). Kfz-Daten werden ausgelesen, um damit das Risiko eines künftigen Versicherungsfalls ermitteln zu können. Dazu werden aus den Daten Rückschlüsse über die Zuverlässigkeit, das Verhalten und den Aufenthaltsort des Fahrzeugführers gezogen.

Da das Ergebnis des Profilings automatisiert weiterverarbeitet werden soll, sind die Anforderungen des Art. 22 DS-GVO zusätzlich zu erfüllen.

Art. 22 Abs. 1 DS-GVO untersagt grundsätzlich Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen, wenn sie dem Betroffenen gegenüber eine rechtliche Wirkung entfalten oder ihn in ähnlicher Weise erheblich beeinträchtigen. Im Umkehrschluss sind maschinelle Entscheidungen erlaubt, die keine solchen gravierenden Folgen haben. Sie stellen keinen Verstoß gegen Art. 22 Abs. 1 DS-GVO dar. Hier hat das Profiling jedoch Auswirkungen auf die Beitragspflichten des Versicherten und ist damit vom grundsätzlichen Verbot der automatisierten Entscheidung umfasst. Auch das Profiling des Verhaltens anderer Fahrer als des Versicherungsnehmers stellt eine Beeinträchtigung „in ähnlicher Weise" dar, darf mithin ebenfalls grundsätzlich nicht zu maschinellen Entscheidungen

führen. Damit müssen die Ausnahmetatbestände des Absatzes 2 geprüft werden, wonach automatisierte Entscheidungen mit ausdrücklicher Einwilligung oder zur Vertragserfüllung zulässig sind. Der Versicherungsvertrag muss also auch einen Passus zur maschinellen Tarifanpassung enthalten. Nachdem dieser nur das Verhältnis zum Versicherungsnehmer abbilden kann (Art. 22 Abs. 2 lit. a DS-GVO), müssen weitere Fahrer explizit einwilligen (lit. c).

Art. 22 Abs. 3 DS-GVO enthält das Recht der betroffenen Person, das Eingreifen einer natürlichen Person der verantwortlichen Stelle in die Entscheidung zu verlangen. Dabei kann diese zur Anfechtung der automatisierten Entscheidung ihren Standpunkt darlegen. Dies erfordert hinreichende Transparenz darüber, dass auf einer automatisierten Entscheidung beruhende Verarbeitung erfolgte, auch wenn diese im Ergebnis nicht belastend war. In diesem Zusammenhang hat die Versicherung Angaben über die verwendete Logik sowie die Tragweite und die angestrebten Auswirkungen zu machen. Für beides ist entsprechend ein Prozess vorzusehen.

Besondere Kategorien personenbezogener Daten dürfen nur nach ausdrücklicher Einwilligung oder auf Grundlage einer speziellen Rechtsgrundlage einem Profiling mit automatisierter Entscheidung unterzogen werden. Je nachdem ob man, wie oben genannt, die Verarbeitung auch von besonderen Kategorien personenbezogener Daten vornimmt, muss für diese ggf. eine Einwilligung eingeholt werden und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der Interessen der betroffenen Personen getroffen werden (Art 22 Abs. 4 DS-GVO).

c) Einbindung der Dienstleister

Zu den Dienstleistern besteht im Zweifel ein Verhältnis der Auftragsverarbeitung. Daher ist mit diesen jeweils ein entsprechender Vertrag nach Art. 28 DS-GVO abzuschließen. Weiterhin müssen die Dienstleister entsprechend sorgfältig ausgewählt und kontrolliert werden. Die Einbindung der Dienstleister bedarf darüber hinaus auf der sog. ersten Stufe keiner weiteren Rechtsgrundlagen.

Weil der erste Dienstleister in Bangladesch und der Unter-Auftragnehmer in den USA sitzen, sind zusätzlich die Anforderungen der Art. 44 ff. DS-GVO zu erfüllen.

Weder im Hinblick auf die USA noch im Hinblick auf Bangladesch gibt es einen Angemessenheitsbeschluss der Kommission im Sinne von Art. 45 DS-GVO. Nachdem es jeweils um die Einbindung eines Dienstleister geht, der nicht zur Unternehmensgruppe der Insight AG gehört, kommen sog. BCR-Controllers als Grundlage im Sinne von Art. 44 ff. DS-GVO für den Datentransfer in die Drittstaaten ebenfalls nicht in Betracht. Gemäß dem Sachverhalt besitzen die Dienstleister zudem keine BCR-Processors. Damit kommen BCR im Sinne von Art. 46 Abs. 2 lit. b, Art. 47 DS-GVO insgesamt nicht als Grundlage der Übermittlung auf der „zweiten Stufe" (Art. 44 ff. DS-GVO) in Betracht.

Die Datenübermittlung könnte jedoch auf andere geeignete Garantien nach Art. 46 DS-GVO oder eine Ausnahme nach Art. 49 DS-GVO gestützt werden. Der EU-Standardvertrag zur Auftragsdatenverarbeitung gemäß Kommissionsbeschluss 2010/87/EU vom 05.02.2010 ist gemäß Art. 46 Abs. 5 Satz 2 DS-GVO als geeignete Garantie im Sinne von Art. 46 Abs. 2 lit. c DS-GVO anzusehen. Die Versicherung müsste mit dem Dienstleister in Bangladesch einen solchen abschließen. Weiterhin müsste der Dienstleister in Bangladesch seinen Dienstleister in den USA anhand der Vorgaben von Klausel 11 des o.g. EU-Standardvertrages als Unterauftragnehmer verpflichten.

4 Durchführung

4.1 Modellierung der Risikoquellen

Nachfolgend werden die Quellen der Risiken für die Rechte und Freiheiten natürlicher Personen identifiziert. Insbesondere wird hierbei bestimmt, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen. Jedoch werden auch die Risikoquellen in Betracht gezogen, die auf eine rechtmäßige Verarbeitung abzielen. Grundsätzlich kann hier zwischen menschlichen und nicht-menschlichen Quellen unterschieden werden.

Interne menschliche Quellen:

- Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler
- Vorsätzliches Handeln: Schaden für den Betroffenen wird entweder billigend in Kauf genommen oder wird vom Verursacher beabsichtigt und stellt Ziel der Handlung dar

Externe menschliche Quellen:

- Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler
- Vorsätzliches Handeln: Angreifer oder Verursacher außerhalb der verantwortlichen Stelle mit dem Ziel der Schädigung des Unternehmens oder der Betroffenen

Nichtmenschliche Quelle:

- Intern/extern: Systemfehler (Software/Hardware) führen zu Verlust, Veränderung oder missbräuchlicher Verwendung personenbezogener Daten

Nachfolgend werden die Risikoquellen für den neuen Telematik-Versicherungstarif modelliert:

- Interner Mitarbeiter – Insight AG
- Externer Mitarbeiter – Bangladesch
- Externer Mitarbeiter – USA
- Versicherter (Kfz-Fahrer)
- Weitere Betroffene (anderer Kfz-Fahrer)
- Sonstiger Dritte (Mitarbeiter Kfz-Werkstatt)
- Softwarefehler
- Hardwaredefekt (physikalisch)
- Umwelteinflüsse (Naturgewalt)

- Cyberkrimineller (Hacker/Schadsoftware)
- Staatliche Institutionen (Nachrichtendienste)
- Staatliche Institutionen (Strafverfolgung)
- Geschäftsführung – Insight AG

Beispiel einer näheren Risikoquellenbetrachtung:

Art der Quelle	Extern/Intern	Unbeabsichtigt/Vorsätzlich	Akteur/Risikoquelle
Menschlich	Intern	Unbeabsichtigt	Mitarbeiter Insight AG
Menschlich	Intern	Vorsätzlich	Mitarbeiter Insight AG
Menschlich	Extern	Unbeabsichtigt	Mitarbeiter (Dienstleister), Sonstiger Dritter
Menschlich	Extern	Vorsätzlich	Cyberkrimineller, Dienstleister, Staatliche Institutionen, Sonstige Dritte
Nichtmenschlich	Intern	-	Hardwaredefekt, Softwarefehler
Nichtmenschlich	Extern	-	Hardwaredefekt, Softwarefehler, Umwelteinflüsse, Gesetzesänderungen, Netzstörung

Abbildung 3: Beispielhafte Risikoquellenmodellierung

4.2 Risikobeurteilung (Risikoanalyse)

Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Die Risiken sollen hinsichtlich der Schwere des Schadens und der Eintrittswahrscheinlichkeit beschrieben werden. Die Risikobeurteilung orientiert sich an den Vorgaben der ISO 31000. Die Risikobeurteilung besteht dabei aus der Risikoidentifikation (I.), der Risikoanalyse (II.) und der Risikobewertung (III.). Zur Risikoidentifikation gehören die Risikobeschreibung samt Risikoquelle sowie der dazugehörige Verarbeitungsgrundsatz nach Art 5 DS-GVO. Die Risikoanalyse umfasst den möglichen Schaden, die Schadenskategorie gem. ErwGr. 75, die Eintrittswahrscheinlichkeit und die Schwere des Schadens. Aus den letzten Punkten ergibt sich dann das Ergebnis der Risikobewertung.

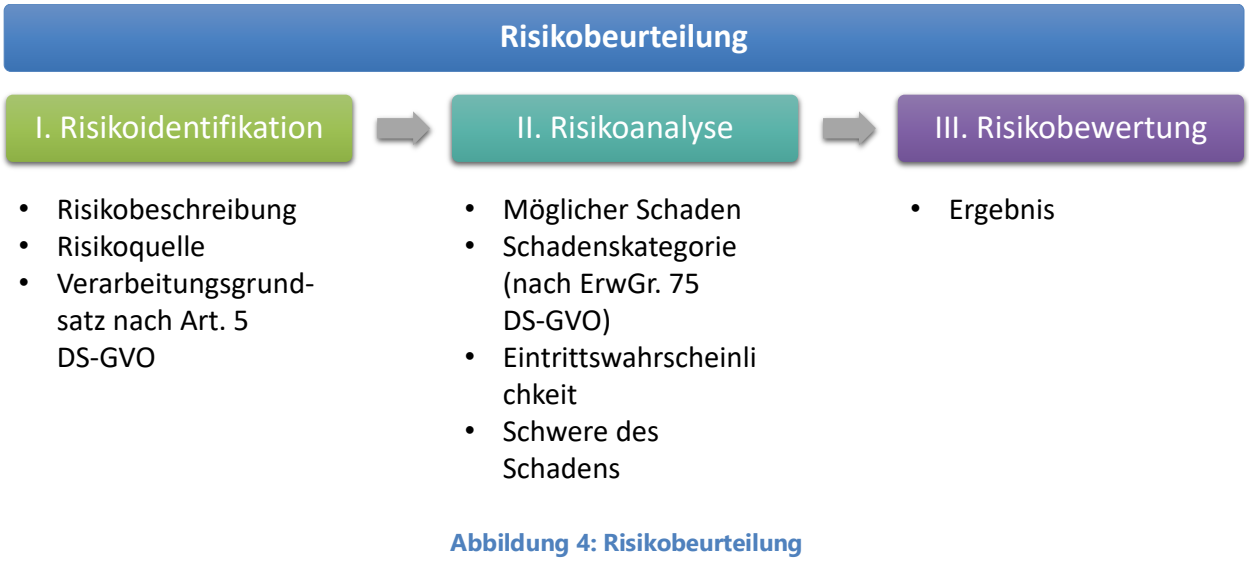


Abbildung 4: Risikobeurteilung

Nachfolgend werden Beispiele für Schadenskategorien nach ErwGr. 75 DS-GVO aufgeführt:

Schadenskategorien
Diskriminierung
Identitätsdiebstahl
Finanzieller Verlust
Rufschädigung
Verlust der Vertraulichkeit bei Berufsgeheimnis
Unbefugten Aufhebung der Pseudonymisierung
Andere wirtschaftliche oder gesellschaftliche Nachteile
Hinderung der Kontrolle der Betroffenen über eigene Daten
Verarbeitung von sensiblen Daten (Eth. Herkunft, Politik, Religion, Sexualleben, Gesundheit, etc.)
Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, Orts-wechsel, etc.)
Verarbeitung von Kinderdaten
Große Menge personenbezogener Daten
Große Anzahl von betroffenen Personen

Tabelle 3: Beispiele für Schadenskategorien nach ErwGr. 75 DS-GVO

Nach dem Schritt der Risikobewertung kann eine graphische Darstellung des Risikos in einer Matrix erfolgen. Nachfolgend ist ein Beispiel hierfür dargestellt:

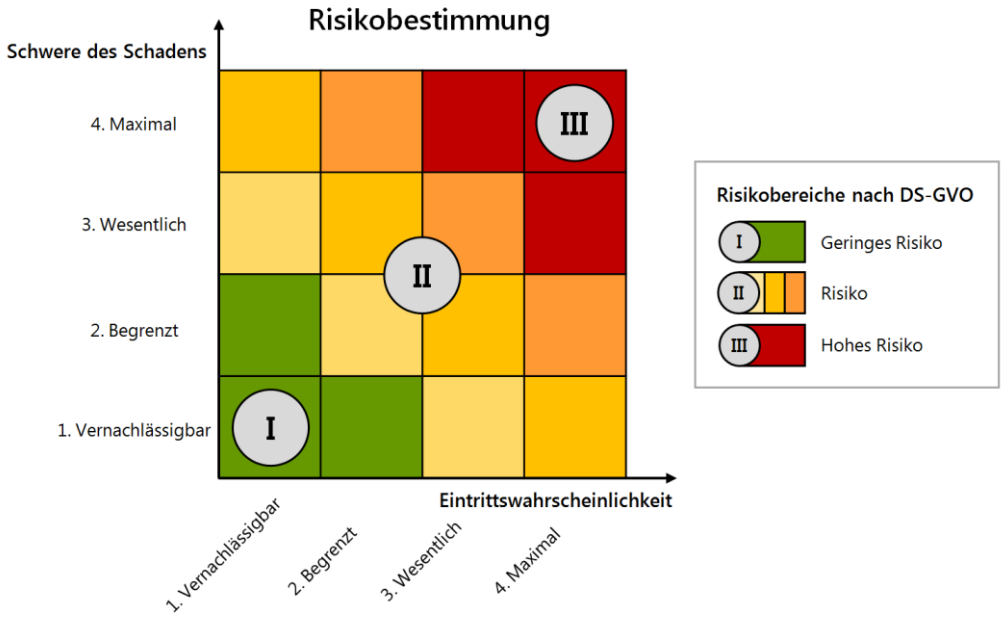


Abbildung 5: Allgemeine Matrix zur Risikobestimmung

Zur Bestimmung der Einteilung/Wertung der Achsen sind folgende Einstufungen sinnvoll heranzuziehen:

Schwere des Risikos

Vernachlässigbar	Kleine Unannehmlichkeiten
Begrenzt	Größere Unannehmlichkeiten
Wesentlich	Wesentliche Folgen
Maximal	Wesentliche und/oder irreversible Folgen

Eintrittswahrscheinlichkeit

Vernachlässigbar	Fast unmöglich / nicht vorstellbar
Begrenzt	Mit gewissem Aufwand machbar (schwierig)
Wesentlich	Mit geringem Aufwand machbar
Maximal	Einfach

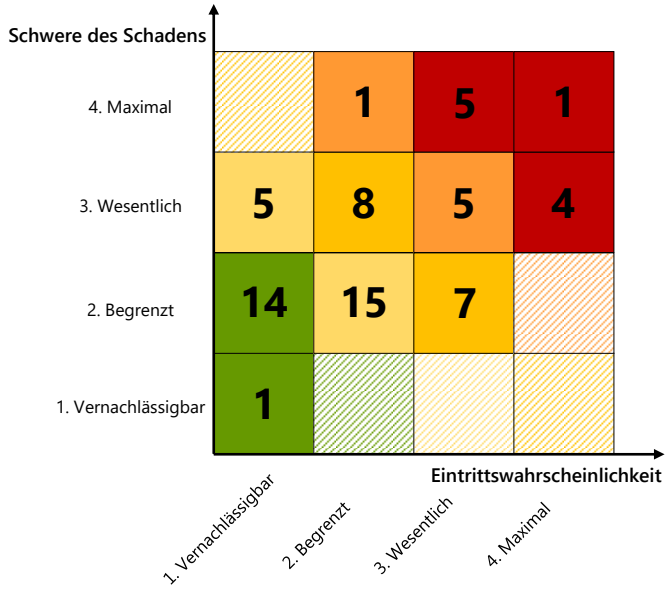
Abbildung 6: Schwere und Eintrittswahrscheinlichkeit

Die komplette Risikobeurteilung für die vorliegende Verarbeitungstätigkeit im Beispielsfall ist in einer separaten Tabelle im Anhang zu finden. Insgesamt wurden 66 Risiken identifiziert und einer Analyse unterzogen. Ein Auszug der Tabelle folgt auf der nächsten Seite.

	Risikobeurteilung (gemäß ISO 31000)							
	I. Risikoidentifikation			II. Risikoanalyse				III. Risikobewertung
Risiko ID	Verarbeitungsgrundsatz (nach Art. 5 DS-GVO)	Risikoquelle	Risikobeschreibung	Möglicher Schaden	Schadenskategorie (nach ErwGr. 75)	Eintrittswahrscheinlichkeit	Schwere des Schadens	Ergebnis
1	Verfügbarkeit	Externer Mitarbeiter - USA	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	Risiko (4)
2	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
3	Verfügbarkeit	Softwarefehler	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	Risiko (4)
4	Verfügbarkeit	Hardwaredefekt (physikalisch)	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
5	Verfügbarkeit	Umwelteinflüsse (Naturgewalt)	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
6	Verfügbarkeit	Externer Mitarbeiter - Bangladesch	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
7	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
8	Verfügbarkeit	Umwelteinflüsse (Naturgewalt)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
9	Verfügbarkeit	Softwarefehler	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	geringes Risiko (2-3)
10	Verfügbarkeit	Hardwaredefekt (physikalisch)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
11	Verfügbarkeit	Versicherter (Kfz-Fahrer)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
12	Verfügbarkeit	Dritter (anderer Kfz-Fahrer)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
13	Integrität und Vertraulichkeit	Externer Mitarbeiter - Bangladesch	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
14	Integrität und Vertraulichkeit	Versicherter (Kfz-Fahrer)	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Begrenzt (2)	Begrenzt (2)	Risiko (4)
15	Integrität und Vertraulichkeit	Dritter (anderer Kfz-Fahrer)	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Begrenzt (2)	Wesentlich (3)	Risiko (5)
16	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
17	Integrität und Vertraulichkeit	Interner Mitarbeiter - Insight AG	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
18	Integrität und Vertraulichkeit	Externer Mitarbeiter - USA	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Begrenzt (2)	Maximal (4)	Risiko (6)
19	Verfügbarkeit	Softwarefehler	Datenpaketverlust zwischen Fahrzeug und DE-CIX-Ki	Einschränkungen beim Auskun	Finanzieller Verlust	Begrenzt (2)	Begrenzt (2)	Risiko (4)
20	Verfügbarkeit	Hardwaredefekt (physikalisch)	Datenpaketverlust zwischen Fahrzeug und DE-CIX-Ki	Einschränkungen beim Auskun	Finanzieller Verlust	Wesentlich (3)	Begrenzt (2)	Risiko (5)
21	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Datenpaketverlust zwischen Fahrzeug und DE-CIX-Ki	Einschränkungen beim Auskun	Finanzieller Verlust	Wesentlich (3)	Begrenzt (2)	Risiko (5)
22	Integrität und Vertraulichkeit	Versicherter (Kfz-Fahrer)	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Vernachlässigbar (1)	Wesentlich (3)	Risiko (4)
23	Integrität und Vertraulichkeit	Dritter (anderer Kfz-Fahrer)	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Vernachlässigbar (1)	Wesentlich (3)	Risiko (4)
24	Integrität und Vertraulichkeit	Sonstiger Dritte (Mitarbeiter Kfz-We	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Begrenzt (2)	Wesentlich (3)	Risiko (5)
25	Integrität und Vertraulichkeit	Softwarefehler	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Begrenzt (2)	Wesentlich (3)	Risiko (5)
26	Integrität und Vertraulichkeit	Hardwaredefekt (physikalisch)	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Begrenzt (2)	Wesentlich (3)	Risiko (5)
27	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Manipulation der Rohdaten im Fahrzeug	"Falsche" Bewertung bei Unfall	Andere wirtschaftliche oder gesellsch	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
28	Integrität und Vertraulichkeit	Interner Mitarbeiter - Insight AG	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persöi	Begrenzt (2)	Begrenzt (2)	Risiko (4)
29	Integrität und Vertraulichkeit	Externer Mitarbeiter - Bangladesch	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persöi	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
30	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persöi	Begrenzt (2)	Begrenzt (2)	Risiko (4)
31	Integrität und Vertraulichkeit	Hardwaredefekt (physikalisch)	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persöi	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
32	Integrität und Vertraulichkeit	Softwarefehler	Manipulation der Mapping-Daten in den Systemen	Falsche Profile, finanzieller Ver	Profilbildung durch Bewertung persöi	Begrenzt (2)	Begrenzt (2)	Risiko (4)
33	Integrität und Vertraulichkeit	Interner Mitarbeiter - Insight AG	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Wesentlich (3)	Begrenzt (2)	Risiko (5)
34	Integrität und Vertraulichkeit	Externer Mitarbeiter - Bangladesch	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Begrenzt (2)	Begrenzt (2)	Risiko (4)
35	Integrität und Vertraulichkeit	Softwarefehler	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Begrenzt (2)	Begrenzt (2)	Risiko (4)
36	Integrität und Vertraulichkeit	Hardwaredefekt (physikalisch)	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
37	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Manipulation der Score-Wert-Daten in den Systeme	Finanzieller Verlust (verfälschte	Finanzieller Verlust	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
38	Richtigkeit	Versicherter (Kfz-Fahrer)	Fehlerhafte Datenübermittlung durch Box aus Kfz	Daten werden nicht oder nicht	Andere wirtschaftliche oder gesellsch	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)

Abbildung 7: Auszug der Risikobeurteilung

Das Ergebnis der Risikobewertung, d.h. die Verteilung der Risiken hinsichtlich der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere, wird nachfolgend dargestellt:



Es wurden somit insgesamt 15 geringe Risiken, 41 Risiken und 10 hohe Risiken bestimmt.

4.3 Auswahl geeigneter Abhilfemaßnahmen

Im Anschluss an die Risikoidentifizierung und -bewertung werden verschiedene Abhilfemaßnahmen bestimmt, die eine hohe Risikobewertungen insoweit reduzieren sollen, dass eine erneute Analyse der Risiken eine akzeptable Risikoeinschätzung ergibt. Nachfolgend werden ausgewählte Abhilfemaßnahmen vorgestellt. Grundlage für die Abhilfemaßnahmen ist der ISO-Standard 29151:2016 (Draft).

Control 1:

Pseudonymisierung

Die Pseudonymisierung personenbezogener Daten ist ein Deidentifizierungsvorgang, bei dem bestimmte Attribute eines Datensatzes gelöscht, generalisiert oder durch bestimmte Kennzeichen ersetzt werden, so dass eine Bestimmung einer Person im Nachhinein nicht mehr oder nur wesentlich erschwert möglich ist.

Einsatz zur Risikoeindämmung:

Anwendung :

Keine Weitergabe der Fahrgestellnummer (VIN) an Dienstleister. Stattdessen wird die eindeutige Box-ID übermittelt. Diese ist der Versicherung bekannt und kann nur von dieser dem Betroffenen zugeordnet werden.

Control 2:

Need-To-Know Prinzip

Das Need-To-Know Prinzip beschreibt eine Zugriffsbeschränkung auf Daten für Mitglieder einer Organisation. Ziel ist es, Zugriffe auf Daten auch bei vollen Zugriffsrechten nur zur Ausführung einer legitimen Tätigkeit zu reduzieren.

Einsatz zur Risikoeindämmung:

Einsatz eines Rechte- und Rollenkonzepts samt Protokollieren von lesenden und schreibenden Zugriffen bei der Insight AG. Protokolldateien werden verschlüsselt gespeichert und können nur mit dem 4-Augen-Prinzip unter Einbeziehung des Datenschutzbeauftragten gelesen werden. Regelmäßige Auditierung der Zugriffsmatrix durch den Datenschutzbeauftragten. Einsatz ebenso bei Dienstleistern – Nachweis durch eine genehmigte Trusted Cloud Zertifizierung nach DS-GVO.

Control 3:

Minimierung der Verkettbarkeit

Die Möglichkeit der Zusammenführung von Inhalten, die zu unterschiedlichen Zwecken erhoben werden, soll minimiert werden.

Einsatz zur Risikoeindämmung:

Annahme:

Besitzt ein Halter mehrere Fahrzeuge mit einzelnen Boxen und separaten Versicherungen, so werden diese nicht zusammen bewertet.

In der Datenbank der Versicherung werden die Box-IDs nicht im Klartext gespeichert. Stattdessen sind AES-256 verschlüsselte Werte abgelegt, die durch ein zugriffsbeschränktes HSM (Hardware Security Modul) von der Anwendungssoftware bei Bedarf einzeln entschlüsselt werden.

Control 4:
Zugriffsbeschränkung bei Weitergabe
Die personenbezogenen Daten werden nur an die beteiligten Stakeholder (Systeme, Menschen) weitergegeben, die diese auch zwingend benötigen. Fokus ist der Risikofaktor „Mensch".

Einsatz zur Risikoeindämmung:
Umsetzung der Control-Klassen 5 (Datenschutzrichtlinie), 6 (Organisation), 7 (Mitarbeiter) der ISO 29151.

Control 5:
Sperrung von Daten
Bei einer Sperrung werden personenbezogene Daten auf Grund möglicher Aufbewahrungsfristen von weiteren Verarbeitungen ausgeschlossen und zugriffsgeschützt archiviert.

Einsatz zur Risikoeindämmung:
Eine Sperrung nicht benötigter Daten (nach Vertragsende) des Versicherten wird auf Seiten der Insight AG routinemäßig durchgeführt.

Control 6:
Löschung von Daten
Die Löschung von Daten umfasst Originale, Kopien und archivierte Datensätze und muss durch verschiedene Verfahren oder Methoden sicher und vollständig erfolgen. Eine Wiederherstellung der Daten darf nicht möglich sein. Ausgenommen von der Löschung sind anonymisierte Daten oder Daten, deren gesetzliche Aufbewahrungsfrist nicht abgelaufen ist.

Einsatz zur Risikoeindämmung:
Umsetzung eines Löschkonzepts nach DIN 66398.

Control 7:
Monitoring des Zugriffs
Ziel eines Monitorings ist es festzuhalten, wann und durch wen ein Datensatz erstellt, verändert, gelesen oder gelöscht wurde. Somit können unberechtigte Datenzugriffe detailliert nachgewiesen werden und eine handelnde Person von einem solchen Vorhaben abgeschreckt werden. Alle Zugriffe werden in Logdateien festgehalten.

Einsatz zur Risikoeindämmung:
Das neu angeschaffte Monitoring Tool „IseeAll" erzeugt geeignete Protokolldateien. Diese werden verschlüsselt gespeichert und können nur mit dem 4-Augen-Prinzip unter Einbeziehung des Datenschutzbeauftragten gelesen werden. Regelmäßige Auditierung der Zugriffsmatrix durch den

Datenschutzbeauftragten. Einsatz ebenso bei Dienstleistern – Nachweis durch eine genehmigte Trusted Cloud Zertifizierung nach DS-GVO.

Control 8:
Verschlüsselung
Einsatz von geeigneten kryptographischen Verfahren zur Transportverschlüsselung (Data at transport), Ruheverschlüsselung (Data at rest) und Inhaltsverschlüsselung (End to end encryption).

Einsatz zur Risikoeindämmung:
Kein eigenes Verschlüsselungsprotokoll.
Stattdessen wird eine HTTPS-Verbindung zwischen Box und Endpunkt beim Dienstleister Bangladesch eingerichtet (4096-Bit, Perfect Forward Secrecy, eigene Client- und Serverzertifikate mit SSL-Pinning). Die Kommunikation zwischen Bangladesch und USA erfolgt mit einer OpenVPN-Verbindung (Zertifikatsbasiert, 4096-Bit). Eine Ruheverschlüsselung der Festplatten des Dienstleisters in Bangladesch wird mit einer LUKS-Verschlüsselung der RedHat-Linux Server umgesetzt. Zusätzlich eine transparente Verschlüsselung des DBMS. Ende-zu-Ende-Verschlüsselung der Backups auf Seiten des Dienstleisters in Bangladesch (OpenPGP 8192-Bit). Die Kommunikation zwischen Versicherung und Dienstleister in Bangladesch erfolgt ebenfalls über obige beschriebene HTTPS-Verschlüsselung des Austauschportals – dieses ist zusätzlich in einen OpenVPN-Tunnel eingebettet.

Control 9:
Löschen von temp-Dateien
Temporäre Dateien können von verschiedenen Anwendungen zu bestimmten Zwecken beispielsweise einer Wiederherstellung erstellt werden. Diese Dateien oder Dokumente können mithin personenbezogene Daten enthalten. Ziel ist es, temporäre Dateien umgehend nach Abschluss der abgearbeiteten Aufgabe der Anwendung zu löschen.

Einsatz zur Risikoeindämmung:
Innerhalb der Box werden Sensordaten und übermittelte Daten nach 5 Minuten gelöscht. Umsetzung der Control-Klassen 8 (Asset-Verwaltung) und 12 (Betriebssicherheit) der ISO29151.

Control 10 (Individuell):
Penetrationstest
Durch umfassende Sicherheitstests werden Schwachstellen im System identifiziert und behoben. Hierbei werden unter Produktionsbedingungen Angriffe von außen simuliert, um mögliche, unbekannte Sicherheitslücken zu erkennen.

Externe Beratung mit Linguisten
Verträge werden von einem Linguisten auf klare und verständliche Sprache geprüft und gegebenenfalls angepasst. Dies soll gewährleisten, dass der Versicherte bei Vertragsabschluss die notwendige Transparenz zur Verarbeitung seiner personenbezogenen Daten erhält.

Risikovermeidung: Löschen

Unter bestimmten Rahmenbedingungen führt eine Anonymisierung der Daten nicht zu einer Risikoreduktion. Anstelle der Anonymisierung könnte als mögliche Senkung der Risikobewertung die Risikovermeidung in Form der Datenlöschung in Betracht gezogen werden.

Risikovermeidung: Verzicht auf nicht erforderliche Werte
Werden nicht erforderliche Daten erhoben, kann durch eine Beschränkung auf die zur Ausübung einer legitimen Tätigkeit erhobenen Daten verzichtet werden, um zusätzliche Risiken zu vermeiden.

Implementierung eines ISMS nach ISO27001
Durch die Implementierung eines IT-Sicherheitsmanagementsystems nach ISO 27001 können grundlegende Maßnahmen zur Erhöhung der Systemsicherheit ergriffen und nachgewiesen werden.

Erneute Durchführung einer Restrisikobewertung ergibt folgende Matrix (Einteilung/Wertung der Schwere des Schadens und der Eintrittswahrscheinlichkeit wie unter Kapitel 4.2 beschrieben):

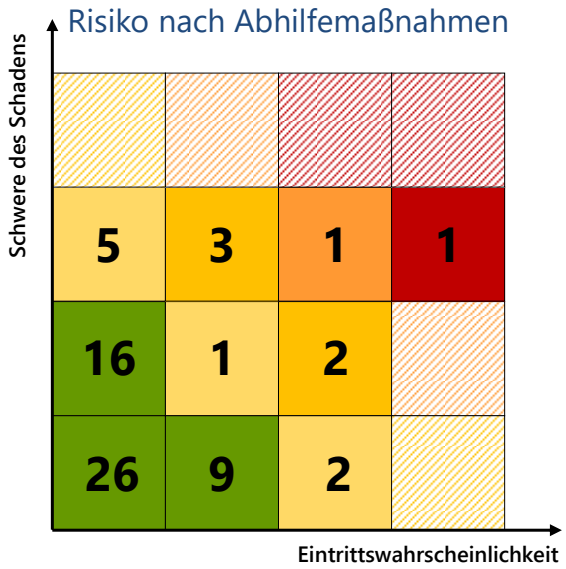


Tabelle 4: Risiko nach Abhilfemaßnahmen

5 Umsetzung

5.1 Umsetzung der Abhilfemaßnahmen

Nachdem das Ergebnis der Risikobewertung feststeht und geeignete Abhilfemaßnahmen zur Bewältigung konkreter Schadensszenarien erarbeitet wurden, müssen sich die Maßnahmen unter realen Bedingungen beweisen. In den meisten Fällen bringen die geplanten Maßnahmen tatsächlich die gewünschte Wirkung und bringen je nach eingesetzten Maßnahmen entweder die Eintrittswahrscheinlichkeit, die Schwere des Schades oder auch beide gleichzeitig in den grünen Bereich der Risikomatrix. Manche Maßnahmen haben jedoch nicht die geplante Wirkung und erfordern Anpassungen durch effizientere Lösungsansätze oder erwirken ein Umdenken bei der Risikobewertung. Manche Maßnahmen können auch die Risken in anderen Bereichen erhöhen.

5.2 Test der Abhilfemaßnahmen

Die Bestätigung, dass eine Abhilfemaßnahme wirklich wirksam ist, bringen gezielte Tests. Auf diese Weise kann man feststellen, ob die Maßnahmen geeignet sind oder nicht und somit gegebenenfalls weiterhin ein hohes Restrisiko besteht. Die erfolgreichen Maßnahmen, die nur noch ein geringes Restrisiko in der Verarbeitungstätigkeit zur Folge haben, entsprechen den Grundsätzen des Art. 5 DS-GVO und können freigegeben werden. Die Verarbeitungstätigkeiten, bei denen jedoch weiterhin ein hohes Risiko besteht, müssen gesondert behandelt werden. Die Bereiche mit einem „normalen" Risiko sollten minimiert werden – wenn keine Maßnahmen vorhanden sind oder diese unter Berücksichtigung der Kosten zu teuer erscheinen, muss dieser Sachverhalt dokumentiert werden.

Nach Durchführung der Datenschutz-Folgenabschätzung und der gezielten Tests hat die Insight AG folgendes hohe Restrisiko festgestellt:

- Risikoquelle: Geschäftsführung
- Risikobeschreibung: Fahrer (ungleich Halter) weiß nichts von der Verarbeitung
- Eintrittswahrscheinlichkeit: Maximal (4)
- Schwere des Schadens: Wesentlich (3)
- Ergebnis: hohes Risiko (7-8)

Da die Insight AG hier keine angemessenen Maßnahmen zur Eindämmung des Risikos festlegen kann, konsultiert sie vor der Verarbeitung die Aufsichtsbehörde entsprechend Art. 36 Abs. 1 DS-GVO. Die Insight AG als Verantwortliche stellt in diesem Zusammenhang entsprechend Art. 36 Abs. 3 DS-GVO der Aufsichtsbehörde folgende Informationen zur Verfügung, um eine Prüfung vornehmen zu können:

- gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
- die Zwecke und die Mittel der beabsichtigten Verarbeitung;
- die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Datenschutz-Folgenabschätzung gemäß Artikel 35 und
- alle sonstigen von der Aufsichtsbehörde angeforderten Informationen

Die Aufsichtsbehörde überprüft die Angaben der Insight AG und kommt ebenfalls zum Ergebnis, dass beim betroffenen Szenario das Risiko als „hoch" einzustufen ist. Als Lösungsansatz, um das Risiko zu minimieren, empfiehlt die Aufsichtsbehörde Fahrzeuge, die mit der entsprechenden Technologie ausgestattet sind, mit für den Fahrer deutlich sichtbaren **Aufklebern** zu kennzeichnen. Somit wird der Fahrer, falls er nicht der Halter des Autos ist, mit notwendigen Informationen versorgt und die Transparenz des Services gewährleistet.

TELEMATIK

Tabelle 5: Vorschlag eines Aufklebers durch die Aufsichtsbehörde

5.3 Dokumentation: Nachweis über die Einhaltung der DS-GVO

Die Insight AG als Verantwortliche kommt der Dokumentations- und Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO durch die Erstellung des DSFA-Berichtes und die Bestätigung der Wirksamkeit der umgesetzten Maßnahmen nach. Nachfolgend wird der Aufbau skizziert:

DSFA-Bericht

- Umfang der DSFA
  - Verarbeitung
  - Übersicht
  - Systemanforderungen
  - Systemarchitektur
  - Wartung und Betrieb
  - Risikokriterien
  - Beteiligte Personen
  - Konsultierte Stakeholder
  - Datenschutzanforderungen
- Risikobeurteilung
  - Risikoquellen
  - Bedrohungen / Eintrittswahrscheinlichkeiten
  - Folgen / Schwere
  - Risikobewertung (Risikomatrix)
  - Compliance-Analyse
- Maßnahmenplan zur Risikobehandlung
- Fazit und Entscheidungen

Tabelle 6: Elemente eines DSFA-Berichts nach ISO 29134