



GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

## Partnerspezifischer Kurzbericht des Verbundprojekts SKINET

Teilvorhaben: Geschützte Methoden für KI-basierte  
Erkennung von Anomalien in automobilen und industriellen  
IT-Netzwerken  
Ausführende Stelle: UA

30.4.2024

---

---

# 1 Aufgabenstellung

Aufgrund der zunehmenden Komplexität und Vernetzung von IT-Systemen ergeben sich neue potenzielle Angriffsvektoren. Eine vollständige Sicherheitsgarantie für Informationen und Betriebsabläufe ist daher praktisch nicht mehr realisierbar. Die fortlaufende Überwachung von IT-Systemen sowie die frühzeitige Erkennung sicherheitsrelevanter Ereignisse sind in heutigen Systemen aufgrund ihrer Komplexität und des damit verbundenen Aufwands nur teilweise durchführbar. Es fehlen dynamische Systeme zur Erkennung und Abwehr von neuartigen Bedrohungen. Neue Angriffsmöglichkeiten entstehen für Angreifer, gegen die bisher nur unzureichend geschützt werden kann. Kontinuierliche Überwachung von Komponenten, frühzeitige Erkennung von Angriffen und umfassende Bewertung des Sicherheitsniveaus des Gesamtsystems sind daher wesentliche Bestandteile einer ganzheitlichen IT-Sicherheitsstrategie. Sobald in diesem Zusammenhang Daten verarbeitet werden, die Informationen enthalten, welche sich auf identifizierte oder identifizierbare natürliche Personen beziehen, greift der Anwendungsbereich des Datenschutzrechts. Dieses dient dem Schutz der betroffenen Personen im Rahmen der Verarbeitung personenbezogener Daten.

Die Bereiche des Datenschutzrechts und der IT-Sicherheit sind eng miteinander verflochten und weisen zahlreiche Überschneidungen sowie potenzielle Zielkonflikte auf. IT-Sicherheit ist einerseits als Grundprinzip des Datenschutzrechts von zentraler Bedeutung, da ohne die Erreichung der Ziele der IT-Sicherheit die Datenschutzprinzipien in der Praxis nur schwer umsetzbar sind. Andererseits führen jedoch IT-Sicherheitsmaßnahmen in vielen Fällen zur Verarbeitung personenbezogener Daten, was insbesondere zu einem Konflikt mit dem Prinzip der Datenminimierung führt. Dies ist vor allem dann der Fall, wenn personenbezogene Daten über ein Netzwerk wie eine KI miteinander verknüpft werden, um zusätzliche Informationen zu gewinnen. Ziel des Projekts war es implizit, diesen Zielkonflikt einer strukturierten Lösung zuzuführen, die beide Teilrechtsgebiete angemessen zum Ausgleich bringt und damit das Gesamtvorhaben rechtmäßig ausgestaltet ist.

Hauptaufgabe des Teilprojektes war es, eben dieses übergeordnete Gesamtprojekt rechtlich zu begleiten, in erster Linie mit Blick auf die datenschutzrechtlichen, haftungsrechtlichen und IT-Sicherheitsrechtlichen Rahmenbedingungen. Im Fokus standen dabei die Beurteilung der personenbezogenen Daten sowie die Haftung im Hinblick auf die Entscheidungs- und Handlungsmöglichkeiten der künstlichen Intelligenz.

# 2 Voraussetzungen und wissenschaftlich-technischer Stand

Die Uni Bremen bzw. später nach Wechsel die Uni Augsburg verfügt über große Erfahrung im Umgang mit Datenschutz und IT-Sicherheitsrechtlichen Fragestellungen und konnte für dieses Projekt u.a. auf die im Projekt DecADE aufgebauten Erfahrungen im Umgang mit der Betrachtung von Cybersicherheitsfällen aufbauen.

### **3 Planung und Ablauf des Vorhabens**

SKINET wurde mit einer Laufzeit von drei Jahren (01.10.2020 - 30.09.2023) geplant. Aufgrund der Corona-Pandemie entstanden Verzögerungen, weswegen das Projekt (kostenneutral) um sechs Monate (bis 31.03.2024) verlängert wurde. SKINET gliederte sich in sieben Arbeitspakete die ein klassisches Wasserfallmodell (Anforderungsanalyse, Systemdesign, Implementierung, Evaluierung) umsetzen. Das Teilprojekt der UA orientierte sich am Ablauf des Gesamtprojekts und in enger Zusammenarbeit mit den Projektpartnern, insbesondere hinsichtlich der jeweiligen rechtlichen Begleitung und Gesamtevaluation.

### **4 Wesentliche Ergebnisse und Zusammenarbeit mit anderen Stellen**

Inhaltlich konnte neue Erkenntnisse zu folgenden wesentlichen Fragen gewonnen werden:

- Identifizierung und Festlegung der juristischen Rahmenbedingungen für die rechtliche Abbildung von künstlicher Intelligenz (KI).
- Erstellung eines internen rechtlichen Leitfadens zur KI, der sich mit IT-Sicherheitsrecht, Datenschutzrecht und Haftungsrecht befasst.
- Vertiefte Untersuchung der Compliance-Anforderungen für die Entwicklung und den Einsatz von KI-gestützten Systemen.
- Analyse der Anforderungen des Produktsicherheitsrechts und des Produkthaftungsrechts im Kontext von KI-Produkten.
- Begleitung der Systementwicklung zur datenschutzrechtlich-konformen Ausgestaltung aller im System verwendeten Technologien im Sinne von Privacy by Design/Default
- Haftungsrechtliche bzw. Beweisführungs-Unsicherheiten im deutschen Recht, die nun auch durch Europarecht parallel zu unseren Erkenntnissen teil geschlossen wurden

Zudem konnte konkret im Datenschutzrecht mithilfe der von uns entworfenen Datenschutztabelle und in Anlehnung an das „Standard Datenschutzmodell“ (SDM) ein Datenschutzkonzept entworfen werden, dass der Komplexität von Datenströmen in KI gerecht wird. Dadurch konnten wir explizit erfassen, welche personenbezogenen Daten an welcher Stelle und von wem verarbeitet wurden und so geeignete Vorkehrungen vorschlagen, um die Rechtmäßigkeit der Datenverarbeitungen sicherzustellen. Diese Tabellen war gleichzeitig auch Fundament für die abschließenden Bewertung der einzelnen Use Cases.



GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

## Partnerspezifischer Abschlussbericht des Verbundprojekts SKINET

Teilvorhaben: Juristische Konformität KI-gestützter  
Sicherheitsmaßnahmen in automobilen und industriellen  
IT-Netzwerken  
Ausführende Stelle: UA

30.04.2024

---

---

<b>Dokument Informationen</b>	
Zuwendungsempfänger	UA
Förderkennzeichen	16KIS1221
Datum	30. April 2024
Vorhabensbezeichnung	SKINET: Proaktive Sicherheit durch Künstliche Intelligenz in automobilen und industriellen IT-Netzwerken
Teilvorhaben	Juristische Konformität KI-gestützter Sicherheitsmaßnahmen in automobilen und industriellen IT-Netzwerken
Laufzeit des Vorhabens	01.10.2020 - 31.03.2024 (36 Monate + 6 Monate Verlängerung)
Berichtszeitraum	01.01.2022 - 31.12.2022

<b>Kontaktinformationen</b>		
Name	Telefon	Fax
Prof. Dr.Benedikt Buchner	e-Mail	
	+49 (0)821 598-4980	
	<a href="mailto:benedikt.buchner@jura.uni-augsburg.de">benedikt.buchner@jura.uni-augsburg.de</a>	

Partner	Kontakt	Telefon e-Mail	Adresse
AVL Software & Functions GmbH (AVL)	Dirk Geyer	+49 941 630 89 135 <a href="mailto:dirk.geyer@avl.com">dirk.geyer@avl.com</a>	Im Gewer- park B29 93059 Regens- burg
b-plus technologies GmbH (B+)	Bernhard Pfeffer	+49 991 270302-724 <a href="mailto:bernhard.pfeffer@b-plus.com">bernhard.pfeffer@b-plus.com</a>	Ulrichsberger Straße 17 94469 Deggen- dorf
Carl Zeiss AG (ZEISS)	Heiko Winkler	+49 7364 20 5538 <a href="mailto:heiko.winkler@zeiss.com">heiko.winkler@zeiss.com</a>	Carl-Zeiss- Straße 22 73447 Oberko- chen
TG alpha GmbH (TGA)	Martin Aman	+49 (0) 991 40 22 71 30 <a href="mailto:m.aman@tgalpha.de">m.aman@tgalpha.de</a>	Ulrichsberger Str. 17 94469 Deggen- dorf
Technische Hochschule Deggendorf (THD)	Prof. Dr. Martin Schramm	+49 991 3615 578 <a href="mailto:martin.schramm@th-deg.de">martin.schramm@th-deg.de</a>	Dieter-Görlitz- Platz 1 94469 Deggen- dorf
Technische Universität München (TUM)	Prof. Dr.-Ing. Georg Carle	+49 89 289 18030 <a href="mailto:carle@net.in.tum.de">carle@net.in.tum.de</a>	Boltzmannstraße 3 85748 Garching bei München
Universität Augsburg (UA)	Prof. Dr. Benedikt Buchner, LL.M.	+49 821 598-4980 <a href="mailto:benedikt.buchner@jura.uni-augsburg.de">benedikt.buchner@jura.uni-augsburg.de</a>	Universitäts- straße 24 86159 Augs- burg
<b>Assoziierter Partner</b>			
Linhardt GmbH & Co.KG (LV)	Stefan Ernst	+49 9942 951 239 <a href="mailto:stefan.ernst@linhardt.com">stefan.ernst@linhardt.com</a>	Dr.-Winterling- Str. 40 94234 Viecht- ach

## Inhaltsverzeichnis

<b>1</b>	<b>Notwendigkeit der geleisteten Projektarbeiten</b>	<b>5</b>
1.1	Motivation . . . . .	5
1.2	Ziele . . . . .	5
1.3	Arbeitsplan . . . . .	6
<b>2</b>	<b>Wesentliche wissenschaftlich-technische und andere Ergebnisse</b>	<b>7</b>
2.1	AP 1 . . . . .	7
2.2	AP 2 . . . . .	7
2.3	AP 3 . . . . .	7
2.4	AP 4 . . . . .	7
2.5	AP 5 . . . . .	8
2.6	AP 6 . . . . .	8
<b>3</b>	<b>Nutzen und Verwertbarkeit der Projektergebnisse</b>	<b>12</b>
<b>4</b>	<b>Die wichtigsten Positionen des zahlenmäßigen Nachweises</b>	<b>12</b>
4.1	Löhne . . . . .	13
4.2	Sachkosten . . . . .	13
4.3	Reisen . . . . .	13
<b>5</b>	<b>Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen</b>	<b>13</b>
<b>6</b>	<b>Veröffentlichungen der Projektergebnisse</b>	<b>13</b>

# 1 Notwendigkeit der geleisteten Projektarbeiten

In diesem Kapitel werden die Notwendigkeit des Forschungsvorhabens SKINET und die Ziele des mit dem Gesamtvorhaben verbundenen Teilvorhabens der UA dargestellt.

## 1.1 Motivation

Aufgrund der zunehmenden Komplexität und Vernetzung von IT-Systemen ergeben sich neue potenzielle Angriffsvektoren. Eine vollständige Sicherheitsgarantie für Informationen und Betriebsabläufe ist daher praktisch nicht mehr realisierbar. Die fortlaufende Überwachung von IT-Systemen sowie die frühzeitige Erkennung sicherheitsrelevanter Ereignisse sind in heutigen Systemen aufgrund ihrer Komplexität und des damit verbundenen Aufwands nur teilweise durchführbar. Es fehlen dynamische Systeme zur Erkennung und Abwehr von neuartigen Bedrohungen. Neue Angriffsmöglichkeiten entstehen für Angreifer, gegen die bisher nur unzureichend geschützt werden kann. Kontinuierliche Überwachung von Komponenten, frühzeitige Erkennung von Angriffen und umfassende Bewertung des Sicherheitsniveaus des Gesamtsystems sind daher wesentliche Bestandteile einer ganzheitlichen IT-Sicherheitsstrategie. Sobald in diesem Zusammenhang Daten verarbeitet werden, die Informationen enthalten, welche sich auf identifizierte oder identifizierbare natürliche Personen beziehen, greift der Anwendungsbereich des Datenschutzes. Dieses dient dem Schutz der betroffenen Personen im Rahmen der Verarbeitung personenbezogener Daten. Die Bereiche des Datenschutzes und der IT-Sicherheit sind eng miteinander verflochten und weisen zahlreiche Überschneidungen sowie potenzielle Zielkonflikte auf. IT-Sicherheit ist einerseits als Grundprinzip des Datenschutzes von zentraler Bedeutung, da ohne die Erreichung der Ziele der IT-Sicherheit die Datenschutzprinzipien in der Praxis nur schwer umsetzbar sind. Andererseits führen jedoch IT-Sicherheitsmaßnahmen in vielen Fällen zur Verarbeitung personenbezogener Daten, was insbesondere zu einem Konflikt mit dem Prinzip der Datenminimierung führt. Dies ist vor allem dann der Fall, wenn personenbezogene Daten über ein Netzwerk wie eine KI miteinander verknüpft werden, um zusätzliche Informationen zu gewinnen. Ziel des Projekts war es implizit, diesen Zielkonflikt einer strukturierten Lösung zuzuführen, die beide Teilrechtsgebiete angemessen zum Ausgleich bringt und damit das Gesamtvorhaben rechtmäßig ausgestaltet ist.

## 1.2 Ziele

Die grundlegende Zielsetzung des SKINET-Projekts bestand darin, die Methoden und Funktionalitäten der Künstlichen Intelligenz (KI) einzusetzen, um sicherheitskritische Vorfälle und deren Ursachen effizient zu erkennen und zu bewältigen. Neben der reinen Benachrichtigung der verantwortlichen Personen im Falle eines Angriffs sollten auch automatisch geeignete Reaktionsmöglichkeiten vorgeschlagen oder eigenständig eingeleitet werden können, um die bestmögliche Sicherheit und Verfügbarkeit zu gewährleisten. Um dieses Ziel zu erreichen, war die Entwicklung eines verteilten Systems mit KI-gestützten Sensoren und einer KI-Engine zur Erkennung und Bewältigung sicherheitskritischer Vorfälle innerhalb des SKINET-Projekts vorgesehen.

Die Arbeit der UA hat sich dabei grob auf zwei Teile aufgeteilt: Die konkrete Projekt-

begleitung und andererseits die Aufbereitung allgemeiner rechtlicher Grundlagen zur Handhabung des Problemkomplexes KI.

Konkret gab es diese Meilensteine als Ziele:

1. Meilenstein M6.1 KI-Leitfaden aus Sicht des IT-Rechts

Fälligkeit: M18

Arbeitspaket: AP6

Geplantes Ziel: Praxisnahe Ermittlung, Aufbereitung und Darstellung der IT-rechtlichen Compliancevorgaben mit speziellen Bezügen zu Datenschutz, IT-Sicherheit und Haftung.

2. Meilenstein M6.2 Beschreibung der rechtlichen Anforderungen / Dokumentation eines Leitfadens

Fälligkeit: M36

Arbeitspaket: AP6

Beschreibung: Juristische Bewertung der ermittelten IT-rechtlichen Grundlagen am konkreten Fall des Forschungsprojekts.

### **1.3 Arbeitsplan**

SKINET wurde mit einer Laufzeit von drei Jahren (01.10.2020 - 30.09.2023) geplant. Aufgrund der Corona-Pandemie entstanden Verzögerungen, weswegen das Projekt (kostenneutral) um sechs Monate (bis 31.03.2024) verlängert wurde. SKINET gliederte sich in sieben Arbeitspakete die ein klassisches Wasserfallmodell (Anforderungsanalyse, Systemdesign, Implementierung, Evaluierung) umsetzen. Das Teilprojekt der UA orientierte sich am Ablauf des Gesamtprojekts und in enger Zusammenarbeit mit den Projektpartnern, insbesondere hinsichtlich der jeweiligen rechtlichen Begleitung und Gesamtevaluation.

Im Verlauf des Projekts, nämlich im August 2022, wechselte die Projektleitung von der Universität Bremen zur Universität Augsburg. Das Fachpersonal wechselte mit, sodass die Projektbegleitung nahtlos und in Personalidentität fortgeführt werden konnte.

SKINET gliederte sich in sieben Arbeitspakete (AP), wobei sich das Teilprojekt der UA eng am Gesamtprojekt orientiert hat.

In AP 1 hat die UA die datenschutzrechtlichen Grundlagen, die sich aus der DSGVO ergeben, zusammengefasst und erarbeitet, betrachtet wurden zudem die weiteren grundlegenden rechtlichen Fragestellungen und Forschungsaufgaben sich aus der Interaktion von Safety und Security in Verbindung mit KI ergeben.

In AP 2 hat die UA die datenschutzrechtlichen Erkenntnisse vertieft, dazu gehörten auch Fragestellungen aus dem Bereich der Anonymisierung und Pseudonymisierung.

In AP 3 hat die UA die Frage der Verantwortlichkeit und Haftung behandelt und sich dem Komplex von Haftung und KI gewidmet.

In AP 4 wurden die Funktionsmuster der technischen Partner – im Hinblick auf die Differenzen der Use Cases – bewertet.

In AP 5 wurden die Ergebnisse der juristischen Bewertung ausgewertet und insbesondere im Hinblick auf die hypothetischen Überlegungen in einem Forschungsprojekt kritisch bewertet.

In AP 6 hat die UA umfassend die juristischen Problemfelder – IT-Sicherheitsrecht, Datenschutzrecht und Haftungsrecht – im Hinblick auf die Grundlagen und die konkreten Probleme im Projekt bewertet.

## **2 Wesentliche wissenschaftlich-technische und andere Ergebnisse**

### **2.1 AP 1**

Im AP 1 wurden zunächst in Abstimmung mit den Projektpartnern die grundlegende Bedeutung von Datenschutzrecht und insbesondere das Konfliktfeld mit KI erläutert. Außerdem wurden die grundlegenden rechtlichen Fragestellungen für das Projekt definiert und zudem weitere Recherchen angestellt. Das ist auch wesentlicher Bestandteil des Meilensteins von AP 6, dem KI-Leitfaden, in dem die rechtlichen Grundlagen definiert wurden.

### **2.2 AP 2**

Im AP 2 hat die UA sich vertiefter mit dem Datenschutzrecht auseinandergesetzt und dabei besonderes Augenmerk auf die Rechtsgrundlagen und Rechtsprechung im Hinblick auf Anonymisierung und Pseudonymisierung gelegt und herausgearbeitet. Insbesondere wurde die Schwierigkeit einer „absoluten“ Anonymisierung thematisiert, weil die Sicherstellung, dass die Daten niemals mit den dahinterstehenden Personen in Verbindung gebracht werden sollte, im konkreten Einzelfall zweifelhaft sein kann.

### **2.3 AP 3**

In diesem AP wurde der Fokus auf die haftungsrechtlichen Fragen im Hinblick auf KI gelegt und zusammen mit den technischen Partnern wurden die Grundzüge der Haftung nach dem Bürgerlichen Gesetzbuch und dem Produkthaftungsrecht besprochen. Dies geschah im Hinblick auf die geplanten Handlungsmöglichkeiten der KI, die aber bis zum Projektende im konkreten Einzelfall unklar blieben. Bezüglich des Datenschutzrechts hat die UA folgende Tabelle für die Anwendbarkeit des Datenschutzrechts entworfen, die von den technischen Partnern für die einzelnen Daten ausfüllen war, um eine umfassende rechtliche Beurteilung der Daten und eine Einordnung, ob diese personenbezogen sind, zu gewährleisten.

Die Datenschutztabelle ist exemplarisch dem Dokument als Anhang beigelegt.

### **2.4 AP 4**

Im AP 4 wurden die Funktionsmuster der technischen Partner sowohl hinsichtlich der datenschutzrechtlichen als auch hinsichtlich der haftungsrechtlichen Problematiken bewertet. Dies geschah auf Basis der aktuellen Planung, konnte aber Unsicherheiten über die zukünftige Verwendung von Daten und auch die Verwendung der Software nicht komplett berücksichtigen. Eine juristische Bewertung erfolgt in der Regel im Einzelfall und solange die Planung noch zu abstrakt blieb, war eine juristische Bewertung nicht immer endgültig

möglich, obgleich versucht wurde, diese Unwägbarkeiten zu berücksichtigen. Für die datenschutzrechtliche Behandlung wurden insbesondere die Rechtfertigungsmöglichkeiten nach Art. 6 der DSGVO untersucht und festgestellt, dass grundsätzlich für alle in Betracht kommenden Datenverarbeitung eine Rechtfertigung über die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO möglich ist. Alternativ könnte in einigen Fällen auch auf eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO abgestellt werden, dabei besteht allerdings das Risiko der Widerruflichkeit.

## **2.5 AP 5**

In diesem AP 5 hat die UA die Funktionsmuster hinsichtlich etwaigen Änderungsbedarfs untersucht. Ein solcher ergab sich – nach dem aktuellen Stand – aber nicht, da die technischen Partner ohnehin kaum personenbezogene Daten verwendeten und auch haftungsrechtlich keine besonderen Risiken bestanden. Insbesondere, da die KI oft keine eigenen Entscheidungen treffen sollte.

Zusammenfassend bestanden zum Schluss – auch auf Basis der rechtlichen Grundlagen – keine rechtlichen Bedenken. Dies ist allerdings nur der Endpunkt des Projekts, klargestellt wurde in-soweit auch, dass sich in der praktischen Nutzung – mit eventuell weitergehenden Daten und Nutzungsmöglichkeiten – neue rechtliche Probleme stellen könnten, die eine erneuten rechtlichen Untersuchung für den konkreten Einzelfall erforderlich machen

## **2.6 AP 6**

Die größte Herausforderung im Hinblick auf die rechtliche Betreuung des Projekts liegt im frühen Entwicklungsstadium der künstlichen Intelligenz und den damit verbundenen Unsicherheiten bezüglich ihrer genauen Ausgestaltung. Juristische Beurteilungen erfordern jedoch präzise Angaben, um fundierte Aussagen treffen zu können. Während des Projektverlaufs war lange Zeit unklar, welche personenbezogenen Daten überhaupt erhoben und genutzt werden sollten, sowie welche Handlungsmöglichkeiten die Software letztendlich haben würde. Dies erschwerte die rechtliche Beurteilung und Begleitung erheblich, da Bewertungen stets anhand konkreter Einzelfälle vorgenommen werden müssen. In den jeweiligen Aufgabenbereichen wurden folgende Ergebnisse erzielt:

### **2.6.1 Task. 6.1.**

In diesem Task werden die juristischen Rahmenbedingungen zur rechtlichen Abbildung von KI ermittelt und fixiert. Einbezogen werden dabei sowohl aktuelle Gesetzgebung, Rechtsprechung, aber auch jüngste Veröffentlichungen aus der juristischen Forschung zu KI. In einer Zusammenschau werden die projektrelevanten Vorgaben gefiltert und praxistauglich dargestellt. Außerdem werden Regulierungsdefizite zur KI ermittelt und darauf basierend rechtliche Lösungsvorschläge ermittelt.

Für die Darstellung der juristischen Rahmenbedingungen wurde eine umfangreiche Recherche durchgeführt, wobei sowohl die aktuellen Regelungen als auch die Gesetzesvorhaben, insbesondere in der Europäischen Union, berücksichtigt wurden. Das Ergebnis dieser

Aufgabe war die Erstellung eines umfassenden rechtlichen Leitfadens zur Künstlichen Intelligenz, der sich insbesondere mit dem IT-Sicherheitsrecht, dem Datenschutzrecht und dem Haftungsrecht befasste.

Als Ausgangspunkt für die Definition von Künstlicher Intelligenz wurde folgende Definition zu Beginn des Leitfadens herangezogen:

"Künstliche Intelligenz (KI) ist ein Bereich der Informatik, der darauf abzielt, Computer und Software so zu entwickeln, dass sie menschenähnliche Intelligenzfunktionen aufweisen. Dazu gehören Lernen, Logik, Problemlösung, Wahrnehmung und die Fähigkeit zur Nutzung von Sprache. (Burbles Pianos, 2019 <https://doi.org/10.1515/iwp-2019-2010>) KI ist eine breite Kategorie, die eine Vielzahl von Unterfeldern umfasst, darunter maschinelles Lernen (ML), Deep Learning, neuronale Netzwerke und kognitive Computing-Technologien. Die KI-Technologie kann entweder eine allgemeine oder spezifische (schwache) Intelligenz aufweisen. Allgemeine KI-Systeme sind jene, die alle intellektuellen Aufgaben, die ein Mensch ausführen kann, erfüllen können, während spezifische oder schwache KI-Systeme nur auf bestimmte Aufgaben ausgerichtet sind." (vgl. KI-Guide)"

Im Anschluss behandelte der Leitfaden ausführlich die Problematiken im Zusammenhang mit den genannten Rechtsgebieten.

Im Datenschutzrecht ist insbesondere das Spannungsfeld zwischen Big Data und Datenschutz relevant. Künstliche Intelligenz benötigt in der Regel eine große Menge an Daten, während das Datenschutzrecht darauf abzielt, personenbezogene Daten zu schützen. Gemäß Artikel 6 der Datenschutz-Grundverordnung (DSGVO) muss stets ein Rechtfertigungsgrund für die Datenverarbeitung vorliegen, sei es die Einwilligung der betroffenen Person oder ein überwiegendes Interesse des Verantwortlichen.

Im Haftungsrecht gelten für KI die allgemeinen zivilrechtlichen Grundsätze. Neben einer Haftung nach dem Produkthaftungsgesetz kann auch eine allgemeine Haftung nach den §§ 823 ff. des Bürgerlichen Gesetzbuches (BGB) in Betracht kommen. Grundsätzlich haftet derjenige, der eine fehlerhafte KI hergestellt hat. Zusätzlich kann eine vertragliche Haftung des Verkäufers bestehen.

Im Hinblick auf das IT-Sicherheitsrecht ist zu beachten, dass Künstliche Intelligenz als Informationstechnik im Sinne des § 2 Abs. 1 BSIG betrachtet wird, da sie alle technischen Mittel zur Verarbeitung von Informationen umfasst. KI-Funktionen müssen daher bestimmte Sicherheitsstandards bezüglich Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen erfüllen, wie in § 2 Abs. 2 BSIG festgelegt. Dazu gehören Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen sowie bei der Anwendung solcher.

Abschließend wurde festgestellt, dass es derzeit keine spezifischen Gesetze zur Künstlichen Intelligenz gibt, jedoch entsprechende Vorhaben seitens der Europäischen Union anstehen. Diese sind jedoch während der Projektlaufzeit nicht in Kraft getreten und wurden daher zunächst nur oberflächlich auf ihren potentiellen Einfluss auf das Projekt untersucht.

### **2.6.2 Task. 6.2.**

Das IT-Recht stellt umfassende Complianceanforderungen an die Entwicklung und an den Einsatz von technischen Systemen. Die Zahl der Regulierungen und deren Granularität variiert dabei je nach Anwendungsbereich. Der Task will deshalb, aufbauend auf den vorherigen Erkenntnissen, diejenigen gesetzlichen Vorgaben ermitteln, die im Projektkontext zwingende Anforderungen darstellen. Insbesondere die umfassende IT-Sicherheitsgesetzgebung der letzten Jahre, zum Beispiel in Bezug auf KRITIS, hat Vorgaben geschaffen, die für eine Vielzahl von Produkten gelten und deshalb sektorübergreifend Bedeutung genießen.

Im Rahmen der Vertiefung der IT-Sicherheitsgrundsätze wurden die genannten Aspekte genauer betrachtet.

Zunächst wurde geprüft, ob die KRITIS-Anforderungen erfüllt sind. Kritische Infrastrukturen sind Organisationen oder Einrichtungen, deren Ausfall oder Beeinträchtigung erhebliche Auswirkungen auf das staatliche Gemeinwesen hätte. Im Projekt wurde die KI zunächst ausschließlich zu Forschungszwecken entwickelt, und geplant war ihr Einsatz lediglich als Software in Fahrzeugen oder in der Industrie im Bereich Verpackung. Da diese Bereiche nicht als kritische Infrastruktur eingestuft werden, spielten die umfassenden KRITIS-Vorgaben im Rahmen des Projekts nach dem aktuellen Kenntnisstand keine Rolle.

Dennoch sollten die Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) gemäß dem Bundesgesetz über die Sicherheit in der Informationstechnik (BSIG) berücksichtigt werden. Insbesondere gewährt das BSIG dem BSI bestimmte Befugnisse, wie z.B. die Möglichkeit, Warnungen gemäß § 7 BSIG auszusprechen.

Für das Projekt war es wichtig, dass die IT-Sicherheit dem allgemeinen Stand der Technik entspricht. Dies bedeutet, dass angemessene Sicherheitsvorkehrungen getroffen werden müssen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten.

### **2.6.3 Task. 6.3.**

Wo einerseits spezielle IT-sicherheitsrechtliche Vorgaben gelten, greifen andererseits die zivilrechtlichen Vorgaben der Produkthaftung und mit dem ProdSichG auch der Produktsicherheit. Gerade das Haftungsrecht bedeutet eine nachgelagerte Kontrolle der Funktionsfähigkeit und Gefahrlosigkeit des Einsatzes von entwickelten Produkten, indem den Entwickler umfangreiche Produktbeobachtungspflichten treffen. Das Themenfeld Produktbeobachtung und KI ist bisher juristisch kaum beforscht. Mit T 6.3 soll deshalb an dieser Stelle ein neuartiges Praxisbeispiel geschaffen werden, das die produktsicherheits- und produkthaftungrechtlichen Anforderungen für KI-Produkte konkret und in enger Kooperation mit den Konsortialpartnern aufzeigt. In diesem Task wurde auf die erarbeiteten Grundlagen zum Haftungsrecht zurückgegriffen und die Risiken der Haftung aufgezeigt und dabei differenziert zwischen der Produkthaftung und der Produzentenhaftung.

Im Ergebnis können die allgemeinen Vorschriften problemlos auch auf KI und ihre Risiken angewendet werden. Der Vorteil des (deutschen) Rechts ist insofern, dass Normen derart abstrakt gehalten sind, dass sie – obgleich zum Teil Jahrzehnte alt – auch problemlos auf neue Sachverhalte anwendbar sind.

So heißt es in § 823 Abs. 1 BGB: Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet. Wenn diese Verletzung eines Rechtsgutes durch eine KI geschieht, haftet derjenige, der kausal für den Schaden verantwortlich ist. Das kann derjenige sein, der sie hergestellt hat, aber auch derjenige, der sie eingesetzt ist.

Letztlich kommt es bei der juristischen Bewertung auf den Einzelfall an und gerade im Bereich der KI dürften sich viele Probleme im Einzelfall auch im Bereich der Kausalität abspielen, eine genaue Prognose hierüber ist allerdings zum aktuellen Zeitpunkt nicht möglich.

Zu beachten sind noch die von der Rechtsprechung entwickelten Grundsätze zur Produzentenhaftung, die eine Haftung des Produzenten beschreibt, der Konstruktions-, Fabrikations-, Instruktionsfehler gemacht hat oder dem Fehler in der Produktbeobachtung vorzuwerfen sind (BGH NJW 2009, 1080 (1081); Looschelders, Schuldrecht BT, 16. Auflage, § 63, S. 543, Rn. 13; Steege, NVZ 2021, 6 (10).

Insbesondere letztere sind für die Haftung wegen KI zu beachten. Für KI spielen die Produktbeobachtungspflichten insbesondere insoweit eine Rolle, als dass sie eine Haftung selbst dann begründen können, wenn die KI zunächst ohne Fehler in den Verkehr gebracht wird, sich danach aber ein schädliches Verhalten anlernt. Dabei ist zwischen aktiven und passiven Produktbeobachtungspflichten zu differenzieren: Während passive Produktbeobachtungspflichten sich darauf beschränken, auf die Reklamation von Verwendern hin zu handeln, verlangt die aktive Pflicht, dass fortlaufend eigene Produkttests, Literaturrecherchen, Vergleiche mit den Sicherheitsergebnissen konkurrierender Produkte und vergleichbare Maßnahmen durchgeführt werden. (Erman/Wilhelmi, BGB, 16. Auflage 2020, § 823, Rn. 119; Steege, NVZ 2021, 6 (11)). So wird es beispielsweise als zumutbar angesehen, dass Kraftfahrzeughersteller infolge ihrer aktiven Produktbeobachtungspflicht Fahrzeugdaten auswerten (Steege, NVZ 2021, 6 (11)).

Für ein etwaiges Inverkehrbringen der Software aus dem Projekt wären demnach auch diese Grundsätze zur Produktbeobachtung zu beachten.

Es bleibt darüber hinaus abzuwarten, wie sich die Haftungsgrundsätze durch die Gesetzgebung der EU im Hinblick auf KI verändern werden.

#### **2.6.4 Task. 6.4.**

Mehr und Mehr werden nur datenschutzrechtlich einwandfreie Produkte auf dem Markt akzeptiert, dies gilt gerade für datenverarbeitende KI. Ergänzend zur allgemeinen Compliance bewertet T 6.4 die gefundenen technischen Lösungsansätze in datenschutzrechtlicher Hinsicht, moniert Nichtkonformität und wirkt auf diese Weise von Anfang an zur Entwicklung eines Systems „Privacy by Design“ hin.

Nach der Erarbeitung allgemeiner datenschutzrechtlicher Grundlagen wurden den technischen Partnern des Projekts Datenschutztabellen vorgelegt, die sie basierend auf ihrem Forschungsstand ausfüllen sollten, um eine erste datenschutzrechtliche Einschätzung vornehmen zu können. Diese Tabellen sahen vor, dass die technischen Partner zunächst

feststellen sollten, ob und welche personenbezogenen Daten überhaupt genutzt werden würden, und in einem zweiten Schritt beurteilen sollten, ob eine Anonymisierung oder zumindest Pseudonymisierung der Daten möglich wäre. Abschließend sollte eine Einschätzung darüber erfolgen, ob die Daten auch außerhalb der EU verarbeitet werden könnten.

Erfreulicherweise kristallisierte sich schnell heraus, dass nur sehr wenige personenbezogene Daten genutzt werden sollten, hauptsächlich Daten von IP-Adressen und möglicherweise Kameradaten des Fahrzeugs. Zumindest eine Pseudonymisierung der Daten wurde allgemein für möglich gehalten, wodurch die datenschutzrechtlichen Bedenken im Hinblick auf eine Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO aufgrund der zu schützenden Rechtsgüter durch das Ziel der KI, nämlich den Schutz von Leib und Leben, gering waren. Es wurde erneut klargestellt, dass eine Anonymisierung der Daten immer die bevorzugte Wahl war, sofern dies keine Beeinträchtigung der Funktionen mit sich brachte. Allerdings litt auch die Bewertung dieses Aspekts des Projekts unter dem frühen Forschungsstadium und der begrenzten Konkretisierung für einen Einsatz auf dem freien Markt. Eine erneute Bewertung des Datenschutzes vor einem möglichen Inverkehrbringen wäre daher zwingend erforderlich.

### **3 Nutzen und Verwertbarkeit der Projektergebnisse**

Im Folgenden werden die Verwertung der Ergebnisse aus SKINET durch weitere Forschung der UA vorgestellt.

Das KI-Recht ist ein großes Thema in der Rechtswissenschaft und auch wenn es mittlerweile schon einige Veröffentlichungen dazu gibt, wird es zukünftig weiteren Bedarf für die Behandlung von Rechtsfragen im Zusammenhang mit künstlicher Intelligenz geben. Insbesondere wenn künstliche Intelligenz noch weiter genutzt und weiterverbreitet wird, werden sich weitere rechtliche Fragestellungen ergeben, die zum Teil konkret von Gerichten gelöst werden, zum Teil aber auch in der Rechtswissenschaft selbst behandelt werden. Die Ergebnisse aus SKINET dienen in diesem Zusammenhang als Grundlage für weitere Veröffentlichungen und Forschungen im Zusammenhang mit KI. Auch zukünftige Forschungsprojekte sind denkbar – insbesondere angesichts der Tatsache, dass die europäische Union ebenfalls konkrete Pläne für die Kodifizierung von „KI-Recht“ hat. In etwaigen Projekten würde die UA dann auf den Erkenntnissen von SKINET aufbauen; denkbar wäre auch eine Erweiterung auf weitere Rechtsgebiete im Zusammenhang mit KI, beispielsweise auch das öffentliche Recht oder das Strafrecht. Zudem werden die gewonnenen Erkenntnisse – auch im Hinblick auf die Bedeutung von KI – auch Eingang in die Lehre an der Universität Augsburg finden und so den Studierenden vermittelt werden. Gerade in datenschutzrechtlichen Vorlesungen lassen sich so auch praktische, aktuelle und konkret-technische Bezüge als Anschauungsbeispiel aus dem SKINET-Projekt extrahieren.

### **4 Die wichtigsten Positionen des zahlenmäßigen Nachweises**

Im Folgenden wird auf den Einsatzzweck der wichtigsten Positionen des zahlenmäßigen Nachweises eingegangen.

## **4.1 Löhne**

Die Lohnkosten ergaben sich zum Großteil für ein Team aus zwei wissenschaftlichen Mitarbeiterinnen, welche beide in Teilzeit und befristet für das Projekt beschäftigt waren und Forschungsarbeiten für SKINET ausführten. Beide wissenschaftlichen Mitarbeiter wurden aufgrund der Vorexpertise und dem IT-Bezug Ihrer parallel laufenden Promotion für das Forschungsvorhaben ausgewählt. Daneben wurden über die Projektlaufzeit verschiedene studentische Hilfskräfte zur Recherche und Unterstützung bei der Forschungsarbeit eingesetzt.

## **4.2 Sachkosten**

Sachkosten ergaben sich vor allem aus der benötigten Literatur beziehungsweise den zur juristischen Arbeit notwendigen Datenbank-Zugängen.

## **4.3 Reisen**

Reisen wurden für eine direkte und effiziente Zusammenarbeit im Projekt durch Konsortialtreffen genutzt. Aufgrund der Corona-Pandemie konnten einige geplante Reisen nicht durchgeführt werden, wobei diese Mittel teils und sinnvollerweise zur kostenneutralen Verlängerung des Forschungsprojekts umgewidmet wurden.

## **5 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen**

Weitere Fortschritte im Bereich der interdisziplinären Zusammenarbeit von Juristen und Technikern auf dem Bereich der Anomalie-Erkennung durch KI sind der UA nicht bekannt.

## **6 Veröffentlichungen der Projektergebnisse**

Die Arbeiten der UA zielten von Beginn an auf die Erarbeitung und Entwicklung eines Gesamtergebnisses ab. Das Ergebnis ist nunmehr ein Datenschutzkonzept, einerseits für den konkreten Anwendungsfall in verschiedenen SKINET-Use Cases, andererseits der abstrakte Leitfadens für eine interdisziplinäre Zusammenarbeit von Technikern und Juristen bei der Entwicklung eines KI-Systems. Die endgültigen Erkenntnisse und Schlussfolgerungen konnten erst zum Abschluss des Projekts, unter Einbeziehung aller relevanten Faktoren, ermittelt werden. Eine vorläufige Analyse und Bewertung sowie vorzeitige Veröffentlichungen wären ohne einen umfassenden Einblick in das gesamte System bzw. alle Datenverarbeitungsprozesse nicht sinnvoll gewesen. Das nun vorliegende Gesamtergebnis in Form der entwickelten Konzepte stellt eine innovative Basis für die geplanten Publikationen von UA dar.

## Schema Anwendbarkeit DSGVO (vereinfacht)

Folgendes zur Verfügung stehendes Datum wird geprüft: \_\_\_\_\_

Was ist unter diesem Datum/Datentyp zu verstehen (z.B. Zeitstempel für XY)?:

### Zur Erläuterung:

Die nachfolgende Tabelle soll für jedes Datum, das der KI potentiell zur Verfügung steht, durchgegangen werden, um eine etwaige datenschutzrechtliche Relevanz bezogen auf die DSGVO zu ermitteln.

Wenn ein Prüfungsschritt aus den Nummern 1 bis 3 richtigerweise mit „Nein“ beantwortet wird, ist die DSGVO von vorn herein auf das Datum nicht anwendbar.

Wenn die Anonymisierung (Schritt 4) möglich ist, ist die DSGVO nach der Anonymisierung nicht mehr anwendbar; bis dahin besteht jedoch eine Anwendbarkeit für z.B. die Erhebung des Datums.

Wenn die Fragen 1 bis 3 mit „Ja“ beantwortet werden, ist die DSGVO grundsätzlich anwendbar. Dann müsste in einem nächsten Schritt geprüft werden, inwiefern die Datenverarbeitung gerechtfertigt ist (dies wird auf Grundlage dieser Tabelle zu einem späteren Zeitpunkt erarbeitet).

Die Fragen 5 bis 7 sind eine erste Grundlage für uns, um damit die Rechtfertigung gutachterlich zu erarbeiten.

Prüfungsschritte	Ja	Nein	Unsicher/ diskutabel	Anmerkungen
				Hier bitte auch einen Hinweis darauf einfügen, ob aus dem Datum eines der folgenden Dinge ableitbar ist: rassische und ethnische Herkunft, politische Meinungen, religiöse oder

				weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person
<b>1. Personenbezogenes Datum (Art. 4 Nr. 1 DSGVO):</b>				
<p>Gesetzliche Definition: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder eine identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die anhand von direkten oder indirekten Merkmalen bestimmt werden kann; Dies geschieht insbesondere über die Zuordnung einer Kennung wie bspw. einem Namen zu einer Kennnummer, zu Standortdaten, einer Online-Kennung oder zu anderen Merkmalen.<sup>1</sup> Dies gilt auch nur für natürliche Personen, d. h. bis zu ihrem Tod.<sup>2</sup> Erfasst sind weder juristische Personen, noch Personenmehrheiten (Vereine).<sup>3</sup></p> <p>Bsp.: Unzweifelhaft = Name, Alter, Herkunft, Geschlecht, genetische Daten, Angaben zur finanziellen Situation, etc...</p>				

<sup>1</sup> Paal/Pauly/Ernst DS-GVO Art. 4 Rn. 3.

<sup>2</sup> BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn.9 ff.

<sup>3</sup> BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn.5.

<p>Sonderfall: IP-Adresse; personenbezogenes Datum, wenn sie vom Provider gespeichert wird und unmittelbar einem Nutzer zuzuordnen ist.<sup>4</sup></p>				
<p><b>2. Personenbeziehbare Daten:</b></p> <p>Personenbeziehbarkeit unterscheidet sich vom Personenbezug nach dem Merkmal der Identifizierbarkeit.<sup>5</sup> Dabei sind alle, dem Verantwortlichen theoretisch zur Verfügung stehenden Mittel, zu beachten, die die Person identifizierbar machen.<sup>6</sup> Sie sind als Unterpunkt der personenbezogenen Daten zu verstehen. Es werden zur näheren Bestimmung weitere Daten benötigt.</p> <ul style="list-style-type: none"> <li>– Direkte Bestimmbarkeit: Die direkte Bestimmbarkeit bedeutet, dass die entsprechenden Daten personenbezogen sind, da sie ohne weiteres, sprich ohne weitere Bemühungen oder Zusatzinformationen, einer bestimmten Person zugeordnet werden können.</li> <li>– Indirekte Bestimmbarkeit: Ist die natürliche Person nicht ohne weiteren (vertretbaren) Mehraufwand und zusätzliche Informationen identifizierbar, sind die angefallenen Daten lediglich personenbeziehbar. Sie sind zwar mit entsprechendem Aufwand auch auf eine natürliche Person beziehbar. Allerdings grenzen sie sich von den personenbezogenen Daten insoweit ab, als dass sie nicht unmittelbar Rückschlüsse auf eine natürliche</li> </ul>				

<sup>4</sup> Paal/Pauly/Ernst DS-GVO Art. 4 Rn.11.

<sup>5</sup> Datenschutzrechtlich macht es keinen Unterschied, ob die Daten personenbezogenen oder personenbeziehbar sind, Paal/Pauly/Ernst, DS-GVO, Art. 4 Rn. 8.

<sup>6</sup> BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn.15.

<p>Person zulassen. Bei den personenbezogenen Daten ist dies hingegen der Fall.</p> <p>Bsp.: Kennnummern, Standortdaten, Flurstücknummern, Hausnummern.</p> <p>Kfz-Daten, wenn sie ausgelesen und durch die Hersteller gespeichert werden, wobei zunächst kein Kundenbezug hergestellt wird. Dieser dann aber bspw. auf Anfrage des Kunden auftritt, wenn er Auskunft verlangt über die über ihn gespeicherten Daten.</p> <p>Sonderfall: IP-Adresse; Eine IP-Adresse kann aber auch als personenbeziehbares Datum gelten, wenn sie von Dritten gespeichert wird und sie nicht ohne zusätzliche Informationen (bspw. durch Tracking, Cookies etc.) auf den Nutzer zurückzuführen ist.</p>				
<p><b>3. Verarbeitung des Datum (Art. 4 Nr. 2 DSGVO):</b></p> <p>Gesetzliche Definition: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von diesen Daten zum Gegenstand hat.</p> <p>Der Begriff der Verarbeitung wird sehr weit verstanden und umfasst eigentlich jede Handlung im Zusammenhang mit personenbezogenen Daten; die gesetzliche Definition ist als</p>				

<p>beispielhafte Aufzählung zu verstehen und nicht abschließend.<sup>7</sup></p>				
<p><b>4. Anonymisierung möglich?</b></p> <p>Anonymisieren ist das Verändern personenbezogener Daten derart, dass die hinter den Einzelangaben über persönliche oder sachliche Verhältnisse stehende betroffene Person nicht bzw. nicht mehr identifiziert werden kann.<sup>8</sup> Es dürfen also keine Rückschlüsse auf die Einzelperson mehr möglich sein. Die DSGVO ist nicht anwendbar!</p> <p>Achtung: Auch die Anonymisierung der Daten selbst ist eine Verarbeitung i.S.d. DSGVO; es bedarf also eines Rechtfertigungstatbestandes.<sup>9</sup></p> <p>Beispiele für Anonymisierungstechniken:</p> <ul style="list-style-type: none"> <li>– <u>Randomisierung</u>  Daten werden im Datenbestand so verändert, dass sie weniger genau sind, wobei jedoch die allgemeine Verteilung aufrechterhalten bleibt (stochastische Verlagerung); Merkmale innerhalb der Datentabelle werden vertauscht, sodass einige von ihnen künstlich mit anderen betroffenen Personen verknüpft werden (Vertauschung); Statt Originaldaten werden Dummyeinträge genutzt, welche die Person, die hinter dem Datum steht, repräsentieren, ohne den</li> </ul>				

<sup>7</sup> Paal/Pauly/Ernst DS-GVO Art. 4 Rn. 20.

<sup>8</sup> Paal/Pauly/Ernst, DSGVO, Art. 4, Rn. 48.

<sup>9</sup> Roßnagel, ZD 2021, 188 (189).

<p>Aussagegehalt der Originalinformation zu verfälschen (Differential Privacy)</p> <ul style="list-style-type: none"> <li>- <u>Generalisierung</u> Hier werden die Merkmale betroffener Personen durch die Veränderung der entsprechenden Größenskala oder -ordnung generalisiert, d.h. durch einen weniger spezifischen Wert ersetzt (d.h. durch die Angabe einer Region statt einer Stadt oder eines Monats statt einer Woche).</li> <li>- <u>Irreversible Löschung von Identifikationsmerkmalen</u>, wie Name, Anschrift, Personenkennzeichen, etc..</li> </ul>				
<p><b>5. Wenn Nein: Warum muss es personenbezogen/beziehbar bleiben?</b></p> <p>Hier bitte eine Erläuterung, wieso es für das Betreiben der KI notwendig ist, die Daten in nicht-anonymer bzw. anonymisierter Form zu nutzen.</p>	/	/	/	
<p><b>6. Wenn keine Anonymisierung möglich: ist wenigstens eine Pseudonymisierung möglich?</b></p> <p>Die Pseudonymisierung unterscheidet sich von der Anonymisierung dahingehend, dass lediglich Daten, die zur Identifikation einer Person genutzt werden können, vom allgemeinen Datensatz getrennt werden (Zwei-Schrank-Prinzip<sup>10</sup>). Bei der Pseudonymisierung besteht immer noch die Möglichkeit, das Identifikationsdatum mit dem Datensatz zu verbinden, um die dahinterstehende Person zu identifizieren.<sup>11</sup> Die DSGVO bleibt anwendbar!</p>				

<sup>10</sup> Michalski, NJW 1996, 1305.

<sup>11</sup> Spyra in Clausen/Schroeder-Printzen, Medizinrecht, 2020, § 23, Rn. 20 f.

<b>7. Ist es denkbar, dass das Datum auch außerhalb der EU verarbeitet wird?</b>				
Bspw. auf Servern außerhalb der EU gespeichert wird o. ä.				