Konzept zum Automatisierten Annotieren Rechtlicher Kommentare an einem DSGVO-Modell

Bachelorarbeit von

Janne Wagner

an der Fakultät für Informatik
KASTEL – Institut für Informationssicherheit und Verlässlichkeit

Erstgutachter:	Prof. Dr. Ralf Reussner
Zweitgutachter:	Prof. Dr. Oliver Raabe
Betreuender Mitarbeiter:	M.Sc. Nicolas Boltz
Zweite betreuende Mitarbeiterin:	Leonie Sterz

10. Juli 2023 – 10. November 2023

Karlsruher Institut für Technologie
Fakultät für Informatik
Postfach 6980
76128 Karlsruhe

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst, und weder ganz oder in Teilen als Prüfungsleistung vorgelegt und keine anderen als die angegebenen Hilfsmittel benutzt habe. Sämtliche Stellen der Arbeit, die benutzten Werken im Wortlaut oder dem Sinn nach entnommen sind, habe ich durch Quellenangaben kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen und dergleichen sowie für Quellen aus dem Internet.

ORT, DATUM

. . . . . .

(Janne Wagner)

Zusammenfassung

Ein Fehler eines Softwareprodukts wird teurer, je später er entdeckt und behoben wird. Das gilt auch für darin enthaltene Verstöße gegen die Datenschutzgrundverordnung. Während diese Problematik sowie der bisher hohe zeitliche Aufwand für interdisziplinäre Zusammenarbeit zwischen Software- und Rechtsexperten in der Softwareentwicklung weithin bekannt ist, existieren wenige Ansätze, den Schwierigkeiten konkret entgegenzuwirken. In dieser Bachelorarbeit wird ein Ansatz vorgestellt, der Softwareentwicklern mittels DSGVO-Kommentierungen an ihrem Softwaremodell ein Grundverständnis zu beachtender Datenschutzaspekte bei der Softwaremodellierung vermittelt. Zu dem Ansatz gehört unter anderem ein Annotationsmechanismus, der die Kommentare automatisiert an einer Instanz eines DSGVO-Modells annotiert. Die Modellinstanz soll in der späteren Praxis vom Softwareentwickler stammen. Durch die Kommentar-Hinweise ist der Entwickler somit bereits während der Erstellung seines Modells in der Lage, auf Datenschutzkonformität zu achten, und dies weitgehend eigenständig, da er die Informationen nicht von einem Rechtsexperten einholen muss. Für Fragen soll dennoch auf ihn zurückgegriffen werden.

Neben der Nutzung des DSGVO-Modells von Boltz et al.(unv.) wird ein Kommentarmodell konzipiert. Diese beiden Modelle werden anschließend in einem Annotationsmodell miteinander verknüpft. Letzteres bildet die Grundlage für die automatisierte Annotation. Werden zwei Instanzen dieser Modelle durch den Annotationsmechanismus geladen, so werden sie, basierend auf vorher festgelegten Merkmalen, zu Paaren zusammengefügt und das Ergebnis wird in Form einer Annotationsliste ausgegeben.

Um die Kommentare nachvollziehbar und insbesondere für den Mechanismus verarbeitbar zu machen, wird zu Beginn ein Konzept zur systematischen Kommentierung bestehenden Rechts entwickelt. Anhand dieses Konzepts wird ein Kommentarkatalog erstellt, welcher als inhaltliche sowie strukturelle Grundlage der Annotationen dient.

Gegenstand dieser Arbeit ist somit die Formulierung einer Reihe von Kommentaren zur DSGVO sowie die Implementierung eines Mechanismus', der die DSGVO-Kommentare den passenden Elementen einer DSGVO-Instanz zuordnet und diese Paare abspeichert. Teil zukünftiger Arbeit bleibt es, die Annotation schließlich an einem Softwaremodell, statt einer DSGVO-Instanz durchzuführen. Dies entspricht dem späteren Praxiseinsatz. Allerdings bedarf dieser Schritt einer vorherigen Transformation des Modells in die zugehörige DSGVO-Instanz. Die Ergebnisse der Arbeit stellen insofern nur ein Basisartefakt für die weitere Erarbeitung des Gesamtziels dar.

Die Implementierung des Ansatzes kann als Machbarkeitsnachweis angesehen werden, ohne einen tatsächlichen Praxiseinsatz zu gewährleisten. Bei der Sichtung verwandter Forschungsliteratur existieren Ansätze, die DSGVO in (Meta-)Modellen darzustellen [16, 20, (unv.) Boltz et al.] sowie zur Bewertung der Datenschutzkonformität nach DSGVO durch automatisierte Methoden [20]. Allerdings existieren noch keine Ansätze zur datenschutzrechtlichen Auskommentierung von Softwaremodellen bzw. von deren Instanzen.

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Motivation

Seit dem 24. Mai 2016 ist die Datenschutzgrundverordnung (DSGVO), die ab Mai 2018 in allen EU-Mitgliedsstaaten und ihren Hoheitsgebieten verbindlich war, in Kraft. Sie löste die bis dato geltende Richtlinie 95/46/EG von 1995, auch Datenschutzrichtlinie genannt, ab. Grund dafür ist die maßgebliche Veränderung der Technologie in den vorangegangenen 25 Jahren, die eine Überprüfung der geltenden Vorschriften nötig machte. Somit wurden durch die DSGVO, neben der Übernahme bereits bestehender datenschutzrechtlicher Konzepte, eine Reihe neuer Konzepte eingeführt. Durch sie kommt es zu umfassenden, komplexen Anpassungen in wirtschaftlichen, gesellschaftlichen, politischen und vor allem informationstechnischen Bereichen. Prozesse der Softwaretechnik müssen in Folge dessen umgestaltet und DSGVO-konform implementiert werden. Im Rahmen der Softwareentwicklung erhält insbesondere Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ Beachtung. Hierzu zählt beispielsweise die Umsetzung von Datenschutzkonzepten während der Entwurfszeit des Systems. Verstöße gegen die Verordnungen der DSGVO kosten Unternehmen bis zu 20 Mio. Euro oder 4% ihres jährlichen globalen Umsatzes sowie unter Umständen ihre Reputation [15]. Neben der gesetzlichen Pflicht ist es somit auch aus unternehmerischer Perspektive essentiell notwendig für erfolgreiche Softwareprodukte, dass sie bereits in frühen Entwicklungsphasen DSGVO-Konformität eingehalten wird und, wo möglich, Datenschutzkonzepte integriert sowie umgesetzt werden [6].

Mängel und Fehler in Softwareprodukten führen zu exponentiell teureren Kosten und ihre Behebung wird gleichermaßen aufwändiger, je später die Fehler erkannt, beachtet und behoben werden [5]. Kommt es beim Softwareprodukt zu datenschutzrechtlichen Verstößen, die bereits durch eine andere Softwaremodellierung hätten verhindert werden können, handelt es sich um solche verhinderbaren Mängeln. Ziel sollte somit sein, bereits in der Entwicklungs- und Konzeptionsphase der Software unterstützende Konzepte bereitzustellen, mittels welcher die Einhaltung der DSGVO erleichtert und schneller nachvollzogen werden kann und die die Entwickler auf potentielle Verstöße und Risiken hinweisen. Ein mögliches Vorgehen ist hierbei, ein inhaltserhaltendes Metamodell der DSGVO zu erstellen, und sie somit auf eine Modellebene mit Softwaremodellen zu transformieren. Aufgrund der Komplexität der DSGVO, die in weiten Teilen der Interpretation bedarf, sowie zusätzlicher Regeln der informatischen Modellierung, stellt diese Modellbildung bereits einen umfassenden Prozess dar. Unter anderem Tom et al. [18] diskutieren diese Problematik. Darüber hinaus sind aufgrund der unterschiedlichen Auslegungs- und Herangehensweisen in der Literatur eine Vielzahl diverser Modellierungen der DSGVO vorzufinden. Siehe hierzu unter anderem Torre et al. [20], Tom et al. [18], Sion et al. [16] und das unveröffentlichte Modell von Boltz et al. Des Weiteren besteht bereits bei grundlegendsten Begriffsbestimmungen wie „natürliche Person“ oder „personenbezogene Daten“ Definitionsspielraum. Die Schwierigkeiten, die schon bei der Interpretation von

Grundbegriffen auftreten, zeugen von der Komplexität der Verordnung. Dementsprechend herausfordernd ist es, DSGVO-Artikel als juristischer Laie erschöpfend zu beachten und umzusetzen.

Zusammenfassend wird deutlich, dass zu einer erfolgreichen Entwicklung DSGVO-konformer Softwarekonzepte sowohl ein fundiertes Expertenwissen im Rechtsbereich als auch im Softwarebereich von Nöten ist, um den Herausforderungen der Datenschutzkonformität gewachsen zu sein. Eine solche Zusammenarbeit zwischen Software- und Rechtsexperten erweist sich in der Praxis als schwierig. Häufig kommt es entgegen der anfangs angestrebten Zusammenarbeit dennoch zu einer separaten, isolierten Erarbeitung. Dies beeinflusst das Endprodukt negativ, da beispielsweise Prozesse länger dauern und höhere Kosten verursachen [16].

In dieser Arbeit wird der Ansatz und die Idee von Boltz et al. [6], eine interdisziplinäre Zusammenarbeit durch ein modellbasiertes Framework zu stärken, als Ausgangspunkt genommen. So steht auch in dieser Arbeit die Verbesserung der Zusammenarbeit im Fokus. Von diesem Punkt ausgehend liegt das Arbeitsziel nun einen Schritt weiter. Durch die Entwicklung eines Annotationskonzepts sollen Softwareentwickler ein Hilfsmittel zur Hand bekommen, mit welchem sie eigenständiger als bisher rechtskonforme Softwareprodukte entwickeln können. Das Konzept soll bereits während der Softwareentwicklung Hinweise darauf geben, wo spätere Datenverarbeitungsprozesse hinsichtlich der DSGVO kritisch verlaufen können und deshalb eine besondere Beachtung verlangen. Darüber hinaus soll die Zusammenarbeit zwischen Rechts- und Softwarebereichen vereinfacht werden, indem die Softwareentwickler ein gestiegenes inhaltliches Grundverständnis, Bewusstsein und eine Sensibilität für Aspekte der DSGVO entwickeln. So können Entwickler selbstständiger arbeiten und sind erst in größeren, abschließenden Fragen auf die Expertise eines Juristen angewiesen. Nicht beabsichtigt ist hingegen die vollständig eigenständige Erarbeitung und Entscheidungsfindung des Entwicklers. Das Annotationskonzept stellt keinen Ersatz der Zusammenarbeit dar.

Für diesen Ansatz wird zu Beginn ein Konzept zum systematischen Kommentieren des bestehenden Rechts entworfen und mittels diesem ein Beispielkatalog von Kommentaren zur DSGVO erstellt. Anhand dieses Katalogs soll es möglich sein, ein Softwaremodell automatisiert mit erforderlichen Datenschutzhinweisen zu annotieren. Neben der erleichterten Fehlerfeststellung durch den Softwareentwickler, dienen diese Hinweise dazu, den Gesetzestext auf für den Rechtslaien verständliche Aussagen zu reduzieren. Bei der Erarbeitung der vorgeschlagenen Methode wird das Metamodell der DSGVO von Boltz et al. (unveröffentlicht) zugrunde gelegt. Abschließend wird sie an einer Instanz eines Fallbeispiels - einer Modellinstanz der Travel Planner Application [3] - getestet.

Mittels dieses Konzepts kann es bereits sehr früh im Entwicklungsstadium der Software zur Beachtung der DSGVO kommen. Das wiederum kann sich positiv auf potentiellen Überarbeitungsaufwand und entstehende Kosten auswirken.

Im nachfolgenden Teil der Bachelorarbeit werden zuerst in Kapitel 2 die Grundlagen dargestellt. Anschließend wird sich im 4. Kapitel mit der Ausarbeitung eines Konzepts zum systematischen Kommentieren bestehenden Rechts befasst. Hier wird zu Beginn ein allgemeines Konzept vorgeschlagen und dieses anschließend auf den Kontext dieser Arbeit spezifiziert. Darauf folgt in Kapitel 5 die Erläuterung des Kommentarmodells, welches sich mit der konkreten Umsetzung des zuvor entwickelten Konzepts im Kontext der

DSGVO auseinandersetzt. Im darauf folgenden Abschnitt 6 wird der entwickelte Annotationsmechanismus vorgestellt, worauf in Kapitel 7 die Auswertung der Annotationen und des Mechanismus' erfolgt. Nach einer kurzen Darstellung verwandter Arbeiten wird abschließend der Blick auf zukünftige Arbeit gerichtet.

2. Grundlagen

In diesem Abschnitt wird ein Überblick über die wesentlichen zugrundeliegenden Inhalte gegeben. Sie dienen als Basis der Entwicklung des Konzepts. Zu Beginn werden rechtliche Grundlagen erläutert, die zur Formulierung der eigens erstellten Kommentierungen hilfreich sind. Daraufhin folgen technische Voraussetzungen aus dem Bereich der modellbasierten Softwareentwicklung.

2.1. DSGVO

Die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ [23] mit dem Kurztitel „Datenschutz-Grundverordnung“ (DSGVO) hat das europäische Datenschutzrecht zum Inhalt. Sie basiert zum einen auf dem „Vertrag über die Arbeitsweise der Europäischen Union“ (AEUV), insbesondere Art. 16 AEUV. Zum anderen auf Art. 8 „Schutz personenbezogener Daten“ der Charta der Grundrechte der Europäischen Union [22].

In der DSGVO sind die Regeln zur Verarbeitung personenbezogener Daten natürlicher Personen festgehalten. Sie dient der EU-weiten Vereinheitlichung im Umgang mit ebendiesen Daten. Neben dem Schutz der Daten und somit der Einschränkung ihrer Verarbeitung wird durch Art. 1 Abs. 3 DSGVO auch der freie Datenverkehr des europäischen Binnenmarktes gewährleistet.

Mit dem 25. Mai 2018 löste die DSGVO die vorangegangene Richtlinie 95/46/EG ab und ist seitdem in der Europäischen Union rechtlich bindend. Zwar hat die DSGVO im Gegensatz zu ihrem Vorgänger verordnenden Charakter und gilt somit unmittelbar in allen Mitgliedstaaten, wodurch eigentlich keine weiteren Umsetzungsmaßnahmen notwendig sind. Allerdings stehen die einzelnen Mitgliedstaaten in der Pflicht, durch „Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß der Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit [...]“ [Art. 85 DSGVO] mit dem nationalen Rahmen in Einklang zu bringen. Hierzu war eine Frist von zwei Jahren einzuhalten, die ab dem Inkraftreten der Verordnung am 24. Mai 2016 begann [24]. Grundsätzlich gelten ausschließlich die Bestimmungen der Verordnung. Es bestehen jedoch einzelne Öffnungsklauseln, die es den Mitgliedstaaten ermöglichen, gewisse Datenschutzaspekte eigenständig zu regeln [10, S. 1]. Diese Umsetzung der Verordnung in nationales Recht sowie die Ausfüllung der Öffnungsklauseln wurde in Deutschland im Rahmen des „Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU“ (DSAnpUG-EU) in einer Neufassung des Bundesdatenschutzgesetzes (BDSG) vereinigt.

Abschließend erlangte die DSGVO am 20. Juli 2018 im gesamten Europäischen Wirtschaftsraum (EWR) Gültigkeit.

2.2. Auslegungsmethodik

Die Auslegung von Gesetzen gehört zu den Kernaufgaben der Rechtswissenschaften. Im Zentrum steht hierbei die Begründung, warum und wie ein bestimmter Begriff im Gesetz verwendet wird - was er umfasst und was nicht. Die Argumente, die für die Auslegung verwendet werden, stammen aus den „vier Tätigkeiten, die vereinigt wirken müssen, wenn die Auslegung gelingen soll“ nach Friedrich Carl von Savigny [11]. Dies sind die grammatische, systematische, teleologische und historische Auslegung. Im unionsrechtlichen Rahmen werden die Methoden nur in wenigen Aspekten different von den nationalrechtlichen angewandt. Folgend sind die Methoden nach Savigny im Einzelnen erläutert:

Grammatische Auslegung: Im Zentrum der sprachlich-grammatischen oder auch philologischen Auslegung steht die Analyse der Syntax und Semantik. Den Maßstab bildet hierbei vordergründig der Sprachgebrauch des Gesetzes, zum Beispiel wie er in Definitionsnormen zum Ausdruck kommt. Da ein Begriff innerhalb eines Gesetzes nicht immer das Gleiche bedeuten muss, kann auch der allgemeine Sprachgebrauch maßgebend sein [11]. Im Zusammenhang der unionsrechtichen Auslegung findet sich hier die Schwierigkeit wieder, dass aufgrund der verschiedenen multilingualen Fassungen von Gesetzen die Auslegung nach dem einzelnen Wortlaut eingeschränkt ist. Nur bei bedeutungsgleichem Wortlaut in mehreren Fassungen kann auf die Bedeutung der Norm geschlossen werden. Durch die *Autonomie des Unionsrechts* ist eine Bedeutungsauslegung eines unionsrechtlichen Begriffs nach nationalem Recht unzulässig [9].

Systematische Auslegung: Diese Kategorie der Auslegungsmethodik bezieht sich auf den Kontext einer Norm. „Es (das systematische Element; Anm.d.Verf) bezieht sich auf den inneren Zusammenhang, welcher alle [...] Rechtsregeln zu einer großen Einheit verknüpft“, so Savigny. Es handelt sich demnach sowohl um einzelne Normen als auch das Normengefüge als Ganzes. Darüber hinaus wird mithilfe der Frage, welches Verhältnis dem Gesetz gegenüber dem Rechtssystem zuteil wird, die Stellung der auszulegenden Rechtsnorm im Textzusammenhang geprüft und die Auslegungsargumentation aufgebaut [11]. Differenzen zur unionsrechtlichen Auslegung bestehen kaum. Auch hier wird die Stellung der Norm im Normengefüge betrachtet. Darüber hinaus ist nun von Bedeutung, ob es sich um ein Sekundärrecht handelt. In diesem Fall wird es in Verbindung mit dem Primärrecht ausgelegt [9].

Teleologische Auslegung: Eine teleologische Argumentation bezieht sich auf den Sinn und Zweck, welcher mit der Rechtsnorm verfolgt wird. Da dies in der Regel jedoch nicht eindeutig feststeht, besteht die Gefahr, dass statt des Gesetzes eigene Zielvorstellungen zugrunde gelegt werden. Somit lässt sich teleologischen Auslegungsargumenten schnell widersprechen. Um dem entgegenzuwirken, werden sie vermehrt in Kombination mit historischen Auslegungen verwendet [11]. Im Zusammenhang mit dem Unionsrecht, fragt die teleologische Auslegung nach den Grundentscheidungen, auf denen die Norm basiert. In diesem Sinne sind die Erwägungsgründe von Bedeutung. Darüber hinaus wird häufig der *effet-utile*-Grundsatz der teleologischen Auslegung

zugeordnet. Demnach sei eine Norm des Unionsrechts so auszulegen, dass sie ihm im Gesamten zu maximaler Wirkung verhilft [9].

Historische Auslegung: Argumente aus dieser Auslegungskategorie beziehen sich auf den geschichtlichen Zusammenhang und somit auf die Abstammungs- und Schöpfungsgeschichte der Rechtsnorm. Des Weiteren sind bei Gesetzen ebenso die zeitlichen Umstände ihrer Entstehung zu betrachten. Darüber hinaus können Erwägungen des erlassenden Gesetzgebers ebenfalls eine Rolle spielen. Außerdem sollte beachtet werden, dass es nicht nur in der Vergangenheit Gründe für die Gesetzeserlassung gab, sondern gegenwärtig auch solche für die Erhaltung sprechen [11]. Die historische Auslegung hält im Unionsrecht einen untergeordneten Stellenwert inne. Dies liegt insbesondere an den anspruchsvollen Mehrheitsentscheidungen, weshalb Streichungen oder die Rückkehr zu früheren Konzeptionen gängig ist [9]. Ausschließlich wenn Unterlagen eine „gesetzgeberische Überzeugung“ [9] aufweisen, können sie als Auslegungstatbestand verwendet werden. Da Erwägungsgründe die wesentlichen Überlegungen des Gesetzgebers wiedergeben, können sie auch in den Bereich der historischen Auslegung fallen.

2.3. Gesetzeskommentare

Um eine Vielzahl von Alltagssituationen erfassen zu können, sind Gesetzestexte in abstrakter Sprache verfasst. Dies führt zu einem großen Spielraum in der Interpretation und inhaltlichen Erfassung des Gesetzestextes. So entstehen insbesondere für Rechtslaien, doch auch für Juristen Herausforderungen bei der praktischen Anwendung. Um dem zu begegnen, befassen sich die Autoren von Gesetzeskommentaren kritisch mit dem Sinn von Gesetzesformulierungen, ihrer Beziehung zu anderen Rechtsnormen und stellen einen Gesamtzusammenhang her. Es handelt sich bei Gesetzeskommentaren insofern um Fachliteratur, die Erläuterungen von Paragraphen und Artikeln eines Gesetzes beinhalten. Die Kommentare stellen dabei eine Unterstützung dar, Gesetze richtig interpretieren und infolgedessen korrekt anwenden zu können. Dadurch ermöglichen sie Lesern diverser Expertisegruppen, ein tiefgründiges Verständnis von Gesetzestexten zu erlangen und dienen beispielsweise als Basis juristischer Entscheidungen.

Bei der Erstellung von Gesetzeskommentaren wird auf diverse Quellen zurückgegriffen. Im Bezug auf die DSGVO werden neben der Auswertung von Rechtsprechungen und der Auslegungsmethodik auch die Erwägungsgründe der DSGVO einbezogen.

Begriffsbedeutung des „Kommentars“ in dieser Arbeit:

Als Teilergebnis dieser Arbeit wird ein Konzept zur systematischen Kommentierung bestehenden Rechts, sowie ein Katalog mit rechtlichen Kommentaren zur DSGVO erstellt. Letztere sollen anschließend an Software-Metamodellen annotiert werden können. Die eigens formulierten Kommentare sind begrifflich vom juristischen Gesetzeskommentar zu differenzieren. Die Kommentare in dieser Arbeit werden als Hilfsmittel zur Erstellung eines Katalogs verwendet, um das bestehende Recht der DSGVO im Kontext der Softwareentwicklung angemessen interpretieren und umsetzen zu können. Sie basieren zum Großteil auf den juristischen Gesetzeskommentaren und sind inhaltlich auf eine Erklärung des

Gesetzesgegenstandes ausgerichtet, jedoch ist eine vereinfachte Darstellung des Inhaltes zentral. Somit sind sie inhaltlich und sprachlich soweit reduziert, dass sie ohne tiefergehendes Rechtsverständnis oder Hintergrundwissen verstehbar sowie anwendbar sind. Insbesondere sind sie auf eine feste Zielgruppe - Softwareexperten - zugeschnitten. Dieser Zielgruppe soll mittels der Kommentierungen ein Grundverständnis der DSGVO-Inhalte vermittelt werden, sodass sie in der Lage sind, es auf Softwareprojekte zu übertragen. Darüber hinaus ist eine Sensibilisierung der Entwickler für rechtliche Problempunkte wünschenswert, sodass offengebliebene Fragen aus Eigeninitiative an den Rechtsexperten formuliert werden können.

2.4. Modellgetriebene Softwareentwicklung

Modellgetriebene Softwareentwicklung wird neben dem Quelltext primär durch Modelle der zu entwickelnden Software charakterisiert. Somit sind zwei Komponenten zu identifizieren: die Programmierung und die Modelle. Letztere sind spezifisch auf die Domäne angepasst und dienen dazu, der Komplexität eines vollständigen Softwareprojekts gerecht zu werden. Jeder Fachbereich bildet hierbei die für ihn relevanten Fragmente in passenden Software-Architekturmodellen ab. Dadurch wird das Ziel, implizites Wissen der Entwickler explizit zu machen, erfolgreich erreicht [14, 2].

Durch diesen modellgetriebenen Ansatz erhalten die Entwickler nicht nur eine modellbasierte Dokumentation ihrer Software, sondern aus den Modellen lässt sich auch ein ausführbarer Quelltext generieren [14]. Der generierte Quelltext fungiert dabei nicht als Ersatz für die klassische Programmierung, sondern wird wiederum als Modell aufgefasst. Ihm wird eine ergänzende Wirkung zuteil [8].

Nach Stachowiak [17, 131ff.] sind Modelle durch die drei Merkmale Abbildung, Verkürzung und Pragmatismus charakterisiert. Sie repräsentieren somit ein Original auf verkürzte Weise und sind einem Subjekt zu einer definierten Zeit und mit einem bestimmten Zweck zugeordnet. Daraus ergibt sich ein Modell-Fragment der realen Welt, welches sich an der intendierten Verwendung orientiert.

Im Fall der modellgetriebenen Softwareentwicklung ergeben sich darüber hinaus ergänzende Anforderungen an die Modelle eines Softwareprojekts. Um einen effektiven Einsatz zu gewährleisten, sollten Modelle gewisse Eigenschaften notwendigerweise aufweisen. Zum einen müssen sie, um der Komplexität zielführend entgegenzutreten, hinreichend abstrahiert sein. Des Weiteren sollten sie für die Verwender verständlich konzipiert sein sowie das Original ausreichend beschreiben. Hierbei gilt es, zwischen einer Reduktion der Attribute im Sinne des Verkürzungsmerkmals auf der einen Seite und der Vollständigkeit des Modells auf der anderen abzuwägen. Dadurch können Vorhersagen über Eigenschaften, die ohne das Modell nicht einsehbar wären, getroffen werden [14]. Der zuletzt genannte Aspekt ist in dieser Arbeit von besonderem Interesse, da anhand der extrahierten Attribute die automatisierte Annotation der Kommentare ausgeführt werden soll.

Erweiternd können Modelle durch Metamodelle beschrieben werden, wobei ein Modell dabei immer eine Instanz des Metamodells abbildet. Es handelt sich also um ein Modell, das ein anderes Modell darstellt und Aufschluss über den Modellierungsprozess gibt. Von Metamodellen können schließlich erneut Instanzen erstellt werden - Meta-Metamodelle.

Dieser Prozess kann fortgeführt werden, bis eine Metamodell-Instanz als selbsterklärend angesehen wird [14]. Bei dem in dieser Arbeit verwendeten DSGVO-Modell handelt es sich um ein Metamodell der Ebene M2 des MOF-Standards [1]. Dahingegen werden die Architekturmodelle, auf denen die Kommentare in der späteren Praxis annotiert werden sollen, auf der M1-Modellebene des MOF-Standards eingeordnet.

Darüber hinaus bieten Architekturmodelle, die während des Software-Designprozesses erstellt werden, einen Vorteil: Aus ihnen können bereits Attribute und Eigenschaften des zukünftigen Systems abgeleitet werden [13, 4]. Insofern liegt es nahe, mittels einer Analyse eines solchen Architekturmodells auch DSGVO-relevante Attribute wie beispielsweise Vertraulichkeit zu entschlüsseln und auszuwerten. Somit können bestimmte Muster erkannt und automatisiert mit Erklärungen, Hinweisen oder möglichen Risiken annotiert werden.

2.5. Metamodell der DSGVO

Für ein Original - in dem hier relevanten Fall die DSGVO - bestehen diverse Möglichkeiten der Darstellung als Modell. Die Unterschiede gehen dabei primär aus der differierenden Gewichtung der zu modellierenden Aspekte hervor. So gibt es auch im Fall der DSGVO-Modellierung verschiedene Varianten. Siehe hierzu unter anderem Torre et al. [20] und Sion et al. [16]. Da der Schwerpunkt dieser Arbeit jedoch nicht auf der Entwicklung oder Bewertung eines konsistenten DSGVO-Modells liegt, wird das in Abbildung 2.1 dargestellte Metamodell der DSGVO von N. Boltz, L. Sterz, C. Gerking und O. Raabe verwendet (unv.)[1].

2.6. EMF - Eclipse Modeling Framework

Das Eclipse Modeling Framework (EMF) [7] ist ein Java-Modellierungsframework. Es eignet sich für diverse Anwendungen, weshalb hier nur die für diese Arbeit relevanten Features aufgezeigt werden.

Als Grundlage eines EMF-Projekts dient ein Domänenmodell - das Ecore-Modell. Es stellt einen spezifischen Problembereich als Klassendiagramm dar, welches vom Nutzer über Editoren erstellt oder editiert werden kann. Um dies zu ermöglichen, basieren Ecore-Modelle auf einem Ecore-Metamodell, welches sich an grundlegende Konzepte der objektorientierten Modellierung hält. Somit fußt EMF auf MOF-Standards [1]. Ausgehend von einer erstellten Modellspezifikation stellt EMF schließlich Tools zur Verfügung, um automatisiert Quellcode zu Ecore-Modellen generieren zu können. Darüber hinaus ermöglicht EMF, aus einem gegebenen Ecore-Modell verschiedene Instanzen des Modells erstellen zu können [7]. In dieser Arbeit werden sowohl Ecore-Modelle erstellt, als auch spezifische Instanzen generiert. Das DSGVO-Modell von Boltz et al. (unv.) liegt bereits als EMF-Projekt vor und kann genutzt werden. Zu diesem wird zu Evaluations- und Validierungszwecken am Ende eine Instanz eines Fallbeispiels erstellt. Darüber hinaus wird ein „Kommentarmodell“ und

[1] Anm.: Das Modell und der zugehörige Programmcode wurden in Englisch verfasst, wohingegen die in dieser Arbeit konzipierten Modelle in deutscher Sprache verfasst sind.

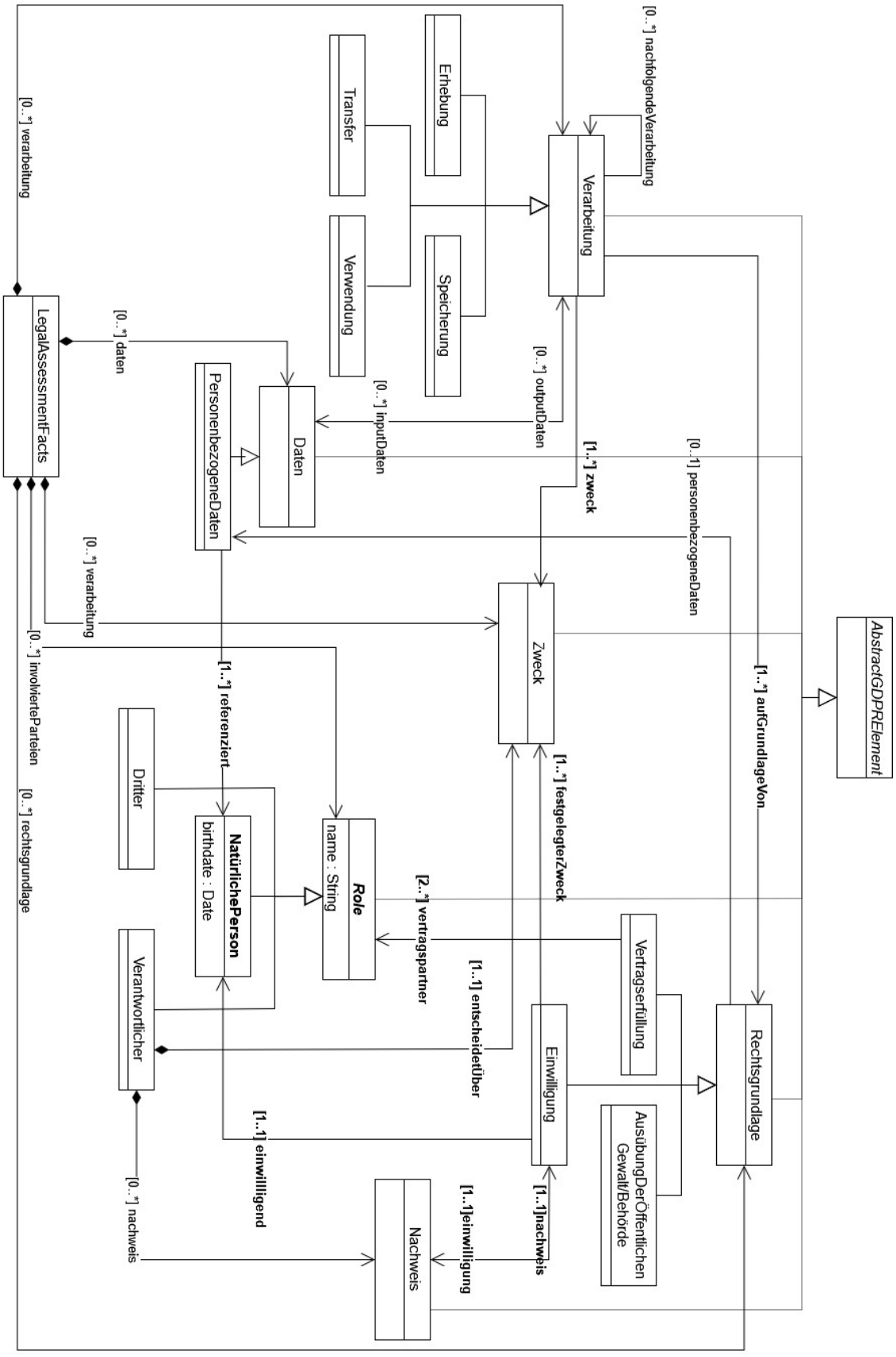


Abbildung 2.1.: DSGVO-Metamodell nach Boltz et al. (übersetzt)

eine zugehörige Instanz erstellt. Sowie ein „Annotationsmodell“, welches die Kommentareinträge den Elementen des DSGVO-Modells zuordnet. Anschließend wird sich die Codegenerierung des Frameworks zunutze gemacht und ein Annotationsmechanismus geschrieben, welcher auf die generierten Modellklassen zugreift.

3. Verwandte Arbeiten

In diesem Kapitel wird ein Überblick über Forschungsarbeiten gegeben, die in thematischem Zusammenhang mit dem vorgestellten Ansatz stehen. Unterschiede zwischen den Konzepten der Literatur und dem in dieser Arbeit vorgestellten Ansatz werden herausgearbeitet. Dadurch entsteht eine Einordnung des Ansatzes in den aktuellen Forschungskontext und der Beitrag, den diese Arbeit leistet, wird erkennbar.

3.1. Model Driven Engineering for Data Protection and Privacy: Application and Experience with GDPR

Torre et al. [20] stellen in ihrem Forschungspapier eine mittels UML und OCL entwickelte holistische, modellbasierte Repräsentation der DSGVO vor. Sie dient als Vorarbeit ihres übergeordneten Ziels: Die Entwicklung automatisierter Methoden zur Überprüfung, Bewertung und Skalierbarkeit der Einhaltung der DSGVO. Aufgrund des teilweisen Einflusses der Mitgliedstaaten auf die DSGVO entwickeln sie einen zweigliedrigen Ansatz. Zum einen konzipieren sie ein generisches DSGVO-Modell, das insgesamt sechs UML-Klassendiagramme umfasst. Es repräsentiert Konzepte und Prinzipien, die auf nahezu alle Kontexte zutreffen sollen und somit Kontextunabhängigkeit beanspruchen. Zum anderen entwerfen Torre et al. ein spezialisiertes Modell, in welchem spezifische Anpassungen der allgemeinen Ebene an bestimmte Kontexte vorgenommen werden. Über diese zwei Ansätze hinaus enthält ihre Arbeit insgesamt vier Artefakte, die in Teilen für diese Bachelorarbeit von Bedeutung waren, da sie unterstützend bei der Erstellung des Kommentarkatalogs wirkten. Insbesondere bei der Auswahl der relevanten DSGVO-Artikel dienten sie als Anhaltspunkt. Zu diesen Artefakten gehören unter anderem (1) eine Tabelle mit Zuordnung der Modellklassen zu den zugrundeliegenden DSGVO-Artikeln, um eine vollständige Rückverfolgbarkeit zu ermöglichen (traceability), (2) ein Glossar, (3) die Beschreibung von 35 Compliance-Regeln, die aus der DSGVO hergeleitet wurden, mitsamt einer Codierung dieser Regeln als Set von Invarianten sowie (4) 20 Variationspunkte, um das generische Modell zu spezialisieren. Darüber hinaus exkludieren Torre et al. in ihrer vorgestellten Modellierung einige DSGVO-Kapitel, die von unzureichendem Einfluss für die Konformitätsprüfung sind. Ausführlich wird dies in Torre et al. [21] begründet.

Zu beachten ist jedoch, dass Torre et al. nicht das Entwickeln datenschutzkonformer Softwaremodelle zum Ziel haben. Vielmehr streben sie die Entwicklung eines AI-assistierten Ansatzes zur Überprüfung der Vollständigkeit von Datenschutzrichtlinien anhand der DSGVO („*An AI-assisted Approach for Checking the Completeness of Privacy Policies Against GDPR*“ [19]) an. Somit geht es um eine automatisierte Prüfung, statt eines Tools für die Softwareentwicklungsphase. Dies sollte bei der Verwendung der Forschungsinhalte aus diesem Paper berücksichtigt werden.

3.2. A Model-Based Framework for Simplified Collaboration of Legal and Software Experts in Data Protection Assessments

Boltz et al. [6] erarbeiten ein modellbasiertes Framework zur verbesserten interdisziplinären Kommunikation zwischen Rechts- und Softwareexperten, um damit einhergehend Datenschutz durch Design (DPbD) sowie die Entwicklung rechtskonformer Systeme zu unterstützen. Somit hat die Arbeit im Sinne der Kommunikationsvereinfachung eine vergleichbare Zielsetzung zu dieser Bachelorarbeit. Allerdings zielt das Konzept der Bachelorarbeit vordergründig auf eine Vereinfachung der Rechtsinhalte der DSGVO, um sie für den Softwareexperten inhaltlich zugänglicher zu gestalten und somit auf eine eigenständigere Arbeitsweise, statt auf eine wechselseitige Kommunikation ab. Darüber hinaus basiert Boltz et al's. Ansatz ebenfalls auf Softwaremodellen, welche den Vorteil haben, dass Qualitätsattribute wie Vertraulichkeit extrahiert und während eines iterativen Prozesses auf ihre Einhaltung gegenüber der DSGVO überprüft werden können. Fehler können daraufhin korrigiert werden, indem das Architekturmodell optimiert wird. Ihre Arbeit geht somit einen Schritt über diese Bachelorarbeit hinaus. Bei dieser ist die Überprüfung der Einhaltung nicht Teil des Annotationsmechanismus.

Während der in dieser Arbeit entwickelte Ansatz auf nur einem Modell von in der Entwicklung befindlicher Software beruht, das annotiert und gegebenenfalls vom Softwareentwickler verbessert wird, verwenden Boltz et al. im iterativen Prozess mehrere Modelle. Zur Überbrückung der Kommunikationsschwierigkeiten kommt ein Transformationsansatz zum Tragen, welcher - vereinfacht dargestellt - ein Softwaremodell in ein „Legal-Assessment-Facts Modell“ transformiert, sodass dieses von Rechts-Experten geprüft und gegebenenfalls verändert werden kann. Anschließend kann das veränderte Rechtsmodell wiederum in ein Softwaremodell transformiert werden. Durch den iterativen Prozess wird eine Möglichkeit gefunden, an frühester Stelle eine DSGVO-Prüfung durchzuführen und diese kontinuierlich mit dem Designprozess fortzuführen [6]. Nachteil dieses Ansatzes könnte sein, dass sich die rechtlichen Aspekte vordergründig auf Art. 6 DSGVO sowie die Grundsätze der Verarbeitung personenbezogener Daten wie Datenminimierung und Zweckbindung nach Art. 5 DSGVO und die Sicherheit der Verarbeitung entsprechend Art. 2 DSGVO beziehen. Diesem Defizit wird mit dem ganzheitlichen Ansatz in dieser Bachelorarbeit begegnet.

3.3. A Model-based Approach to Realize Privacy and Data Protection by Design

Einen weiteren modellbasierten Ansatz zur Realisierung von Datenschutz durch Technikgestaltung beschreiben Pedroza et al. [12]. Die von ihnen vorgestellte Methode beschäftigt sich insbesondere mit den Aspekten der Erkennung und Re-Identifikation personenbezogener Daten sowie der Modellierung und Bewertung des Schutzes der Privatsphäre.

Im Gegensatz zu bereits existierenden Ansätzen, die sich auf die automatische Detektion personenbezogener Daten in Datenbanken ausrichten, konzentrieren sich Pedroza et al.

auf Datenschutzverletzungen im Zusammenhang mit externen Datenquellen. Es werden Wahrscheinlichkeiten berechnet, mit denen ein Datenbankattribut personenbezogene Daten enthält. Um anschließend die resultierenden Verlinkungsrisiken einzuschätzen, wird Open Linked Data verwendet. Diese wird auf identifizierbare Individuen durchsucht, die in Verbindung mit Attributkonzepten der Ausgangsdatenbank stehen. Somit kann die entwickelte Methode Verknüpfungen zwischen Personen und Datenbankkonzepten herstellen.

An dieses Konzept anschließend stellen Pedroza et al. zum einen ein datenorientiertes Modell vor, das zur Erfassung der untersuchten Datenstrukturen und zur weiterführenden Analyse verwendet wird. Es enthält unter anderem die erkannten personenbezogenen Daten in Form von Metadaten. Zum anderen wird ein prozessorientiertes Modell vorgestellt, das zur Erfassung der Datenströme dient. Die anschließend vorgenommene Bewertung der beiden Modelle orientiert sich an etablierten Standards wie ISO-27550 und geht auf die Design-Strategien „Minimieren, Separieren, Abstrahieren, Verstecken“ für den datenorientierten Bereich sowie „Informieren, Kontrollieren, Durchsetzen, Demonstrieren“ im prozessorientierten Bereich ein. Von Bedeutung für zukünftige Arbeiten an dem Ansatz der Bachelorarbeit könnte der integrierte Ansatz der Benachrichtigungen („Notifications“) im Falle einer Datenschutzverletzung sein. Hier instanziieren Pedroza et al. ein Benachrichtigungs-Muster („Notification-Pattern“), in welchem der Softwareentwickler zwischen verschiedenen Optionen und Fällen der Benachrichtigung wählen muss. Zum einen kann das hier verwendete Muster („Pattern“) in Bezug auf die Entwicklung des eigenen Konzeptes genauer angeschaut werden. Zum anderen verdeutlicht Pedroza et al's. Ansatz die Relevanz eines Grundverständnisses der DSGVO bei Softwareentwicklern. Nur wenn das benötigte Verständnis vorhanden ist, kann an entsprechender Stelle die richtige Prozessverarbeitung ausgewählt werden.

4. Konzept zur systematischen Kommentierung bestehenden Rechts

Im folgenden Abschnitt wird ein Konzept zur systematischen Kommentierung bestehenden Rechts eingeführt. Das Konzept soll als Mittel dienen, eine einheitliche, zusammenfassende Darstellung von Gesetzesinhalten zu ermöglichen. Hierzu steht der Verfasser - im Zusammenhang dieser Arbeit wird der Standpunkt eines Rechtslaien eingenommen - vor der Aufgabe, anhand vorher festgelegter Bedingungen zu entscheiden, welche Informationen tatsächlich relevant für den späteren Anwendungskontext sind und welche über das notwendige Maß hinausgehen. Anschließend verfasst er auf dieser Basis einen Kommentar[1]. Vereinfacht wird diese Aufgabe, wenn dem Verfasser durch das Konzept eine gewisse Struktur vorgegeben wird und er dadurch auf Aspekte aufmerksam gemacht wird, die zu nennen wichtig sind. Damit einhergehend folgt die Kommentierung festgelegten Mustern, wodurch die Inhalte begründet zustande kommen.

Konzepte im Allgemeinen dienen zur Umsetzung von Lösungsansätzen hinsichtlich eines konkreten Problems. Das hier verlangte Konzept zur systematischen Kommentierung bestehenden Rechts soll optimalerweise allgemeingültig und auf diverse Rechtstexte anwendbar sein. In diesem Sinne geht es mittels den folgend erläuterten Konzeptansätze darum, ein allgemeines Vorgehen zu entwickeln, wie bestehendes Recht systematisch kommentiert werden kann. So sollen Nutzer (insbesondere Rechtslaien) die resultierenden Kommentare in ihre Arbeit integrieren können und die Gesetzestexte sollen ihnen von einer verständlicheren Seite zugänglich gemacht werden. Durch die Zusammenstellung der wichtigsten Inhalte wird ihnen ein erheblicher Arbeitsaufwand abgenommen. Nach Möglichkeit soll das Konzept eine Form aufweisen, welche es unter anderem ermöglicht, die Kommentare an einem Softwaremodell automatisiert annotieren zu können. Dafür müssen sie eine einheitliche Struktur aufweisen, die sich systematisiert abfragen lässt.

4.1. Allgemeines Konzept

Zu Beginn stellt sich die Frage, welchem Ziel das hier modellierte Konzept im Gesamten dienen soll. Angedeutet wurde dies bereits: Rechtstexte oder auch nur einzelne Rechtsnormen sollen in einem beziehungsweise mehreren Kommentar[en] verständlich zusammengefasst werden. Damit dies gelingen kann, ist es wichtig, zu Beginn die Zielgruppe der Kommentierungen festzulegen. Denn unter anderem vom Vorwissen oder der Anwendung der Kommentare in der Praxis hängt ab, wie Erläuterungen formuliert werden müssen oder welche Einzelbestandteile das Kommentar-Konzept enthalten sollte. Des Weiteren ist es

[1] Ein Kommentar ist das gesamte Konstrukt bestehend aus der Erläuterung und den weiteren Bestandteilen wie Artikel, Begriffe etc.

von Bedeutung, in welchem situativen Kontext das Konzept angewendet wird. Ist es nur von Relevanz, dass Gesetzesnormen erläutert werden, damit sie verstanden werden oder ist darüber hinaus erwünscht, dass dargelegt wird, warum eine bestimmte Norm existiert? Sollen Verfahren, Sanktionen und Ausnahmen mit einbezogen werden oder ist dies für die Zielgruppe irrelevant beziehungsweise besteht die Gefahr einer Überforderung aufgrund zu vieler Details? Kann es dann alternativ sinnvoll sein, solche Informationen implizit als Verweise zu verlinken?

Diese Fragen sollten beantwortet werden, bevor das Konzept für einen konkreten Fall spezifiziert wird. Dies bedenkend kann dennoch ein Konzeptansatz entwickelt werden, der einen allgemeinen Ausgangspunkt ermöglicht, von welchem aus je nach Bedarf weitere Verfeinerungen getätigt werden können.

Um diese Ziele zu berücksichtigen, erscheint es sinnvoll, das Konzept zur systematischen Kommentierung an drei Hauptaspekten auszurichten. Sie gelten unabhängig der letztlichen Konkretisierung und stehen somit für ein allgemein anwendbares Kommentierungskonzept. Die drei Aspekte seien formuliert als:

1. Verstehen eines rechtlichen Konzepts im Ganzen sowie seiner Einzelteile durch aussagekräftige Erläuterungen.
2. Ermöglichung der Rückverfolgung von Erläuterungen und Bereitstellung von Hilfsmitteln zur weiterführenden Recherche.
3. Einordnung der Einzelbestandteile in den Gesetzestext und Darstellung des Gesamtzusammenhangs durch Querverweise sowie Hierarchiedarstellung.

Aus diesen Aspekten lassen sich nun die einzelnen Elemente eines systematischen Kommentars festlegen. Um dem ersten Punkt gerecht zu werden, steht zu Beginn die Extrahierung der Grundelemente der zu kommentierenden Rechtsnorm. Sie werden im Folgenden als *„Grundelement der Rechtsnorm“* bezeichnet. Die einzelnen Elemente werden in strukturierter Weise, orientiert an ihren Bezügen zueinander, genannt sowie verständlich erläutert. Die *„Erläuterung“* ist hierbei der zentrale Bestandteil eines Kommentars. In ihm werden alle relevanten Informationen für den Leser dokumentiert. Konkrete Formulierungen und deren Genauigkeit hängen wiederum von der späteren Zielgruppe ab. Da es sich bei der Erläuterung nicht nur um eine Reformulierung des Gesetzestextes handeln soll, sondern eine Verständlichmachung von ebendiesem, bietet sich die Zuhilfenahme von weiteren Quellen wie Gesetzeskommentaren oder Erwägungsgründen (ErwG) an. Diese beinhalten ausführliche, von Experten formulierte Interpretationen bzw. Begründungen der Rechtsnorm, wodurch sie verständlicher werden. So besteht nun unabhängig der vorhandenen Expertise die Möglichkeit, eine Erläuterung der Norm im systematischen Kommentar zu verfassen.

Zur Berücksichtigung des zweiten Aspekts, der Rückverfolgbarkeit und Transparenz der Erläuterungen, werden die Kommentare durch eine Angabe der Gesetzesartikel, aus denen die Informationen für die Erläuterungen gewonnen wurden, ergänzt. Dabei repräsentieren sie nicht in erster Linie Quellenbelege, sondern verweisen auf die Primärinformationsquelle. Hierbei kann es sich neben einem Rechtskommentar auch um weitere Rechtsquellen handeln. Bezeichnet wird dies im Konzept mit *„Artikel zur Rückverfolgbarkeit“*.

Des Weiteren werden in den Erläuterungen Rechtsbegriffe verwendet, die als potentiell unbekannt eingestuft werden. Diese werden gesondert definiert. Der Übersicht halber

könnte im Kommentar unter *„Verknüpfte Begriffe“* lediglich auf den Begriff referenziert und dieser anschließend in einem Glossar erläutert werden. Das erweist sich insbesondere dann als praktisch, wenn ein zu definierender Begriff wiederholt in verschiedenen Erläuterungen vorkommt. Durch die Referenz auf das Glossar werden doppelte Definitionen in den Kommentarerläuterungen vermieden.

Darüber hinaus bietet es sich an, ebenfalls auf verwandte Rechtsartikel, Erwägungsgründe oder Gesetzeskommentare zu verweisen. Unter der Kategorie *„Verknüpfte Artikel“* kann dies umgesetzt werden. Sie sind von den oben genannten „Artikeln zur Rückverfolgbarkeit“ zu trennen und beziehen sich auf in der Erläuterung genannte, weiterführende Artikel.

Beinhaltet die zu kommentierende Rechtsnorm darüber hinaus aufeinander aufbauende Elemente, sollten diese hierarchischen Zusammenhänge auch in den Kommentaren erkennbar sein. Hier bietet es sich an, die übergeordneten Elemente als solche in den untergliederten Fragmenten über *„Verknüpftes Grundelement der Rechtsnorm“* zu vermerken. Doch auch Bezüge unabhängig der Hierarchie können vermerkt werden. So werden Zusammenhänge verdeutlicht, die ergänzend zu den Erklärungen wirken und ein übersichtliches Gesamtbild sowie einen Einblick in den Gesamtzusammenhang vermitteln.

Diese drei Referenzen werden im Konzept unter der Kategorie *„Verweise“* zusammengefasst. Im Einzelnen untergliedern sie sich in *„Verknüpfte Begriffe“*, *„Verknüpfte Artikel“* und *„Verknüpftes Grundelement der Rechtsnorm“*.

4.2. Mögliche Ausgestaltung des Konzepts

Im Anschluss an das vorgestellte Grundgerüst bleibt die Frage zurück, ob und wie die Formulierung der Erläuterung eines Kommentars systematisch angeleitet werden kann. Dies würde dem unerfahrenen Verfasser eine weitere Stütze geben sowie für Einheitlichkeit sorgen. Ein Blick auf das Zustandekommen rechtlicher Gesetzeskommentare hilft hierbei weiter. Diesen Kommentaren liegt eine umfassende Auslegungsmethodik zugrunde, wie sie in Abschnitt 2.2 eingeführt wurde. Somit wäre eine Überlegung, diese Methodik auch hier einfließen zu lassen. Da jedoch zu Gesetzbüchern bereits in großem Umfang und vielfacher Ausführung Kommentare bestehen, in welche die Auslegungsmethodik bereits eingeschlossen wurde, erscheint es nicht sinnvoll, als Laie die Arbeit von Experten zu wiederholen und erneut eine Auslegungsmethodik für die relevanten Aspekte der DSGVO anzufertigen. Vielmehr sind Bezüge auf die bestehenden Gesetzeskommentare und die Übernahme von Interpretationen daraus sinnvoll.

Da die Auslegungsmethodik allerdings einen großen Anteil am Verständnis für das Zustandekommen von Interpretationen und Erläuterungen hat, könnte es sinnvoll sein, die Auslegungsmethodik der Gesetzeskommentare nicht nur implizit in die Erläuterung einzubeziehen, sondern sie für den Leser explizit sichtbar zu machen. So kann ihr eine stärkere begründende Wirkung auf die Erläuterungen zuteil werden und sie sorgt dadurch beim Nutzer für erhöhtes Verständnis und Hintergrundwissen. Wird beispielsweise im Rahmen der systematischen Auslegung aufgezeigt, wie sich eine Norm im Zusammenspiel mit anderen Normen im Gesamtgefüge verhält, wird der umfassende Wirkungszusammenhang einer Norm ersichtlich. So wären auch die Beziehungen von Sachverhalten in der

praktischen Realwelt, die gegebenenfalls unterschiedliche Normen tangieren, vom Nutzer leichter auf Korrektheit zu überprüfen.

Im Folgende wird ein Beispiel eines modellierten Kommentars mit dem oben genannten Konzept ausgeführt. Die Auslegungsmethodik wird hier explizit einbezogen. Um dies nicht nur auf der Metaebene zu beschreiben, sondern präzise auszuformulieren, wurde ein konkretes Beispiel aus der DSGVO gewählt.

Grundelement der Rechtsnorm:

- Rechtsgrundlage

Artikel zur Rückverfolgbarkeit:

- Art. 5; Art. 6; Komm.[2]: Art. 5 Rn. 6; Komm.: Art. 6 Abs. 1 Rn. 10; Komm.: Art. 6 Abs. 1 Rn. 24

Kommentar:

Grammatische Auslegung: Aufgrund der Position und Funktion innerhalb der Norm geht die Auslegung der Begriffe „personenbezogene Daten, Verarbeitung, Verantwortlicher, Einwilligung " auf die Begriffsbestimmung in Art. 4 DSGVO zurück.

Systematische Auslegung: Die Rechtmäßigkeit der Datenverarbeitung und damit die Formulierung von Rechtsgrundlagen stellt einen zentralen Bestandteil der DSGVO dar. Die Gestaltung eines Rechtsrahmens für die Verarbeitung personenbezogener Daten wird dadurch geschaffen. Der Blick auf übergreifende Regelungsmuster wie beispielsweise auf die Differenz von privaten und öffentlichen Stellen, die Verarbeitung personenbezogener Daten oder des Regelungselements der Erforderlichkeit ist notwendig, um ein Verständnis für die Norm zu entwickeln [26, Art. 6].

Teleologische Auslegung: Der für die Rechtsgrundlage maßgebliche Art. 6 DSGVO basiert auf den Erwägungsgründen 39-50 der DSGVO. Insbesondere ErwG 40 „Rechtmäßigkeit der Datenverarbeitung" sowie ErwG 41 „Rechtsgrundlagen und Gesetzgebungsmaßnahmen" scheinen von Bedeutung. Die übrigen Erwägungsgründe sind Ausgangspunkt für die einzelnen Unterabsätze sowie Literale.

Historische Auslegung: Art. 6 Abs.1 DSGVO geht aus der Vorgängerregelung Art. 7 DSRL hervor, mit dem Unterschied der grundsätzlich geltenden unmittelbaren Bindung. Ergänzt wurde bspw. in Art. 6 Abs. 1 UAbs. 1 lit. f, dass Minderjährige als besonders schutzbedürftige Betroffene gelten. Die Inhalte von Art. 6 Abs. 2 sind auf die Forderung verschiedener Mitgliedstaaten für „größere Flexibilität im öffentlichen Sektor" [26, Art. 6 Rn. 7] zurückzuführen.

Erläuterung: *Grundsatz der DSGVO ist das generelle Verbot einer Verarbeitung personenbezogener Daten, sofern sie nicht durch einen Erlaubnistatbestand einer Rechtsvorschrift legitimiert ist* (Verbot mit Erlaubnisvorbehalt). *In der Rechtsgrundlage wird die Tragweite und Anwendung der Datenverarbeitung personenbezogener Daten dargelegt. Sie muss so präzise geregelt sein, dass sie für den Betroffenen voraussehbar ist und der Zweck der Verarbeitung muss eindeutig daraus hervorgehen*

[2]Dies steht als Abkürzung für Gesetzeskommentar.

sowie festgelegt sein. Je nach zugrundeliegendem Rechtmäßigkeitstatbestand ist sie durch Unionsrecht oder das Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, festgelegt. Für eine rechtmäßige Verarbeitung personenbezogener Daten müssen zum einen die „Grundsätze der Verarbeitung personenbezogener Daten" eingehalten werden. Für diese Einhaltung besteht eine Rechenschafts- sowie Nachweispflicht durch den Verantwortlichen. Zum anderen muss einer der sechs Rechtmäßigkeitstatbestände pro Verarbeitungszweck erfüllt sein. Zu beachten ist, dass eine Einwilligung als Rechtmäßigkeitstatbestand nicht eingeholt werden darf, wenn auch ein anderer Rechtmäßigkeitstatbestand greifen würde. Darüber hinaus gelten Rechtmäßigkeitsanforderungen wie bspw. Betroffenenrechte (Art. 12-23 DSGVO) oder Datensicherheitsmaßnahmen (Art. 32-39 DSGVO). Ausnahmen dieser Rechtsgrundlage sind nur im Rahmen besonderer Verarbeitungssituationen (Art. 85 ff. DSGVO) durch Rechtsvorschriften der Mitgliedstaaten möglich.

Verweise:

Verknüpfte Begriffe:

- Rechtmäßigkeitstatbestände
- Ausnahmefälle der Übermittlung an Drittländer
- Prüfung Zweckvereinbarkeit
- Grundsätze der Verarbeitung
- Nachweis/ Rechenschaftspflicht

Verknüpfte Artikel:

- Art. 12-23; Art. 32-39; Art. 45; Art. 46; Art. 85-91

Verknüpfte Grundelemente der Rechtsnorm:

- -

Zugehörige Glossareinträge:

- *Siehe Anhang A.2*

Es wird deutlich, dass die Hinzunahme der Auslegungsmethodik den Umfang des Kommentars stark erhöht. Es stellt sich die Frage, inwieweit sie einen tatsächlichen Mehrwert für die Anwendung des Kommentars in der Praxis darstellt. Kann der Nutzer mit den zusätzlichen Informationen arbeiten, oder fehlt ihm dazu weiteres juristisches Wissen? Es könnte sogar passieren, dass die resultierende Informationsmenge zu hoch ist, sodass das Ergebnis in der praktischen Anwendung letztlich geringer ausfällt als ohne Auslegungsmethodik. Einerseits wird dadurch mehr Hintergrundwissen vermittelt und eine höhere Nachvollziehbarkeit erzielt. Dadurch wird ersichtlich, wie der Experte zu seiner Interpretation gekommen ist und warum sie in die formulierte Erläuterung übernommen wurde. Andererseits erhöht sich der Umfang maßgeblich. Wie bereichernd ist dieses „Mehr" an Hintergrundinformationen für den Nutzer in der Praxis tatsächlich? Hier muss abgewogen werden zwischen minimal notwendiger Information und möglicher Überinformation, die die Effektivität senken könnte. Ist die Darlegung des Zustandekommens einer Interpretation für die angestrebten Zwecke tatsächlich notwendig?

Dazu noch einmal ein Blick auf das Ziel der Kommentare. Dieses sollte sein, den Nutzern (z.B. Softwareentwicklern) ein wesentliches inhaltliches Grundverständnis, Bewusstsein

und eine Sensibilität für Aspekte des jeweiligen Rechtskonzepts zu vermitteln, wodurch eine selbstständigere Arbeit möglich sein soll (siehe 1). Ist es für dieses Ziel erforderlich, dass zusätzlich zu einer umfassenden Erläuterung tiefgehende Begründungen des Zustandekommens ebendieser angeführt werden? Betrachtet man einen potentiellen Anwendungskontext wie die Softwareentwicklung, so besteht die Hauptaufgabe für den Softwareentwickler in der Entwicklung von Softwaremodellen. In dieser sollen die Kommentare als ein „Tool “ zum Einsatz kommen. Das bedeutet wiederum, dass der Entwickler nicht den Großteil seiner Zeit dem Verstehen und Hinterfragen des Kommentars widmet. Der Kommentar soll eine Unterstützung sein und gerade den zeitintensiven Austausch mit Rechtsexperten reduzieren. Der Einbezug der Auslegungsmethodik würde hingegen vor der ersten Nutzung der Kommentare eine Einführung des Softwareentwicklers in eben diese Methodik nach sich ziehen, damit er die Auslegung auch korrekt einordnen kann. Somit scheint ein ausführlicher, verständlicher Kommentar ohne Auslegungsmethodik zielführender. Insbesondere da Verweise auf weiterführende Aspekte und zugrundeliegende Quellen angegeben werden, werden dem Nutzer die Möglichkeiten mitgegeben, eigenständig offenen Fragen nachzugehen. Des Weiteren lässt sich ein Mittelweg darin finden, bei dringendem Bedarf bestimmte Aspekte der Auslegungsmethodik in die Erläuterung mit einzubinden, dies jedoch nicht als Standard zu betrachten.

4.3. Konkrete Umsetzung des Konzepts in dieser Arbeit

Aufgrund der dargelegten Begründung wurde sich dazu entschieden, beim Konzept zur systematischen Kommentierung bestehenden Rechts im Rahmen dieser Arbeit auf die explizite Ausführung der Auslegungsmethodik zu verzichten. Stattdessen wird sie bei Bedarf implizit eingebunden. Die konkrete Umsetzung des Konzepts besteht aus einem Kommentar welcher zugehörige Unterelemente besitzt. Diese sind: die Nennung des Grundelements der Rechtsnorm, mindestens einem Artikel zur Rückverfolgbarkeit, die Erläuterung als zentralem Element sowie Verweisen. Letztere bestehen aus verknüpften Begriffen, Artikeln oder Grundelementen. Darüber hinaus kann es sich bei Artikeln sowohl um Gesetzesartikel, als auch Gesetzeskommentare oder Erwägungsgründe handeln. Da es sich bei den „Verknüpfte[n] Begriffe[n]“ um Rechtsbegriffe handelt, deren Bedeutung definiert werden muss, werden die Kommentare durch ein Glossar erweitert. Es enthält eben jene Begriffe, auf die referenziert wurde sowie deren Erläuterung und zugehörige Rechtsartikel.

Für die festgelegte konkrete Ausführung des Konzepts in dieser Arbeit ergibt sich nun folgender modifizierter Kommentar zu dem oben angeführten Beispiel. Der Unterschied besteht im Großteil im Weglassen der explizit ausgeführten Auslegungsmethodik:

Grundelement der Rechtsnorm:

- Rechtsgrundlage

Artikel zur Rückverfolgbarkeit:

- Art. 5; Art. 6; Komm.: Art. 5 Rn. 6; Komm.: Art. 6 Abs 1 Rn. 10; Komm.: Art. 6 Abs. 1 Rn. 24

Erläuterung: *Grundsatz der DSGVO ist das generelle Verbot einer Verarbeitung personenbezogener Daten, sofern sie nicht durch einen Erlaubnistatbestand einer Rechtsvorschrift legitimiert ist* (Verbot mit Erlaubnisvorbehalt). *In der Rechtsgrundlage wird die Tragweite und Anwendung der Datenverarbeitung personenbezogener Daten dargelegt. Sie muss so präzise geregelt sein, dass sie für den Betroffenen voraussehbar ist und der Zweck der Verarbeitung muss eindeutig daraus hervorgehen sowie festgelegt sein. Je nach zugrundeliegendem Rechtmäßigkeitstatbestand ist sie durch Unionsrecht oder das Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, festgelegt. Für eine rechtmäßige Verarbeitung personenbezogener Daten müssen zum einen die „Grundsätze der Verarbeitung personenbezogener Daten" eingehalten werden. Für diese Einhaltung besteht eine Rechenschafts- sowie Nachweispflicht durch den Verantwortlichen. Zum anderen muss einer der sechs Rechtmäßigkeitstatbestände pro Verarbeitungszweck erfüllt sein. Zu beachten ist, dass eine Einwilligung als Rechtmäßigkeitstatbestand nicht eingeholt werden darf, wenn auch ein anderer Rechtmäßigkeitstatbestand greifen würde. Darüber hinaus gelten Rechtmäßigkeitsanforderungen wie bspw. Betroffenenrechte (Art. 12-23 DSGVO) oder Datensicherheitsmaßnahmen (Art. 32-39 DSGVO). Ausnahmen dieser Rechtsgrundlage sind nur im Rahmen besonderer Verarbeitungssituationen (Art. 85 ff. DSGVO) durch Rechtsvorschriften der Mitgliedstaaten möglich.*

Verweise:

Verknüpfte Begriffe:

- Rechtmäßigkeitstatbestände
- Ausnahmefälle der Übermittlung an Drittländer
- Prüfung Zweckvereinbarkeit
- Grundsätze der Verarbeitung
- Nachweis/ Rechenschaftspflicht

Verknüpfte Artikel:

- Art. 12-23; Art. 32-39; Art. 45; Art. 46; Art. 85-91

Verknüpftes Grundelement der Rechtsnorm:

- -

Zugehörige Glossareinträge:

- *Siehe Anhang A.2*

5. Kommentarmodell

Um im späteren Verlauf den Annotationsmechanismus implementieren zu können, muss im Vorhinein ein Kommentarmodell konzipiert werden. Das Modell und insbesondere dessen Instanzen bilden die Grundlage der Annotationen.

Für die Modellierung des Kommentarmodells sowie deren Instanzen wurde das Eclipse Modeling Framework (EMF) [7] verwendet. Das Kommentarmodell basiert auf dem zu Beginn in Kapitel 4 entwickelten Konzept zur systematischen Kommentierung bestehenden Rechts. Im ersten Schritt wurde ein Meta-Kommentarmodell erstellt, welches die einzelnen Elemente eines Kommentars enthält. Es ist sozusagen eine Modellierung des in Kapitel 4 beschriebenen Konzepts. Im darauf folgenden Schritt wurde daraus ein Instanz-Modell erzeugt, welches konkret auf die DSGVO bezogen ist. Es leitet, ausgehend von den Bestandteilen des DSGVO-Modells nach Boltz et al., die einzelnen Grundelemente der Rechtsnorm *DSGVO* ab. Zu den Grundelementen wurden schließlich die konkreten Kommentare verfasst. Sie sollen ein späteres Softwaremodell aussagekräftig annotieren, weshalb sie inhaltlich auf diese Zielgruppe und diesen Anwendungskontext begrenzt wurden. Auch wenn das Kommentarmodell im zweiten Schritt auf ein Rechtsmodell - wie hier das DSGVO-Modell - angewandt wird, steht es grundsätzlich für sich allein und ist auch ohne diese Beziehung vollständig funktionsfähig.

5.1. Meta-Modell

Das Kommentarmodell ist auf der Meta-Modellebene angesiedelt und stützt sich in seinem Grundgerüst auf das Konzept zur systematischen Kommentierung bestehenden Rechts. Es ist grundsätzlich nicht spezifisch für die DSGVO konzipiert, sondern in differenten Rechtskontexten, die das identische Ziel der Kommentierung verfolgen, einsetzbar.

Die zugrundeliegende Idee des Kommentarmodells besteht darin, dass ein Kommentar eine einzelne Annotation für das spätere Softwaremodell repräsentiert. Demzufolge muss er alle relevanten Elemente enthalten, die für einen Softwareentwickler in seiner praktischen Arbeit von Bedeutung sind und anhand derer er sein Projekt möglichst eigenständig datenschutzkonform gestalten kann. Durch den Kommentar bereitgestellte Inhalte müssen demzufolge nicht nur direkte Informationen enthalten, sondern schließen auch Verweise auf erwähnte Begriffe, weiterführende Artikel oder verwandte rechtliche Konzepte mit ein. Es ist ersichtlich, dass die spezifischen Anforderungen an den Annotations-Kommentar mit denen des Konzepts zum systematischen Kommentieren übereinstimmen. Aus diesem Grund wird das Konzept übernommen und muss nun nur noch in ein Modell transformiert werden, um für den Annotationsmechanismus verwendet werden zu können.

Die einzelnen Elemente des Konzepts, wie sie in Kapitel 4 bereits in allgemeinen Zügen erläutert wurden, finden sich nun im Modell genauso wieder. Sie sind im Folgenden

erneut erläutert, an dieser Stelle nun aber konkret auf das Gebiet der Softwareentwicklung und die DSGVO bezogen. Das Kommentarmodell ist im zugehörigen Ecore-Diagramm in Abbildung 5.1 dargestellt. Beim Betrachten der Abbildung fällt bereits auf, dass kein *Glossar* modelliert wurde, wie es im Konzept zur systematischen Modellierung eingeführt wurde. Das liegt daran, dass die *Verweise* durch Beziehungen dargestellt werden können und somit keine gesonderte Klasse benötigt wird. Des Weiteren sind die Erläuterungen der Begriffe als Attribut an den Begriff geknüpft, weshalb keine gesonderte Modellierung notwendig ist.

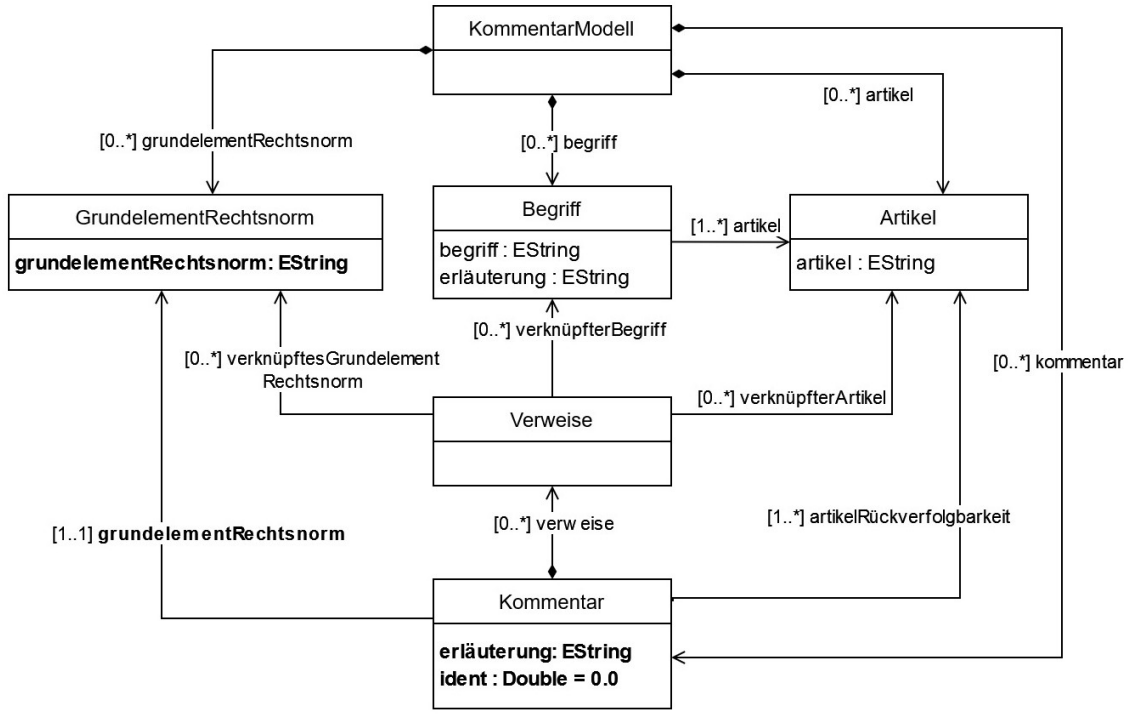


Abbildung 5.1.: Kommentarmodell

Im Folgenden werden die einzelnen Bestandteile des Kommentarmodells beschrieben. Aus genannten Gründen weisen sie eine hohe Ähnlichkeit zu den Bestandteilen des Konzepts zur Kommentierung auf. Allerdings handelt es sich im Modell um einzelne Elemente, die in Beziehung zueinander stehen. Erst die Zusammenstellung der Elemente erzeugt einen Kommentar.

Vorweggenommen sei die Erläuterung der Klasse *KommentarModell*, da sie kein Element des Kommentars im eigentlichen Sinne darstellt. Es handelt sich hierbei um ein Überelement, welches dazu dient, alle weiteren Elemente des Modells zu beinhalten. Somit übernimmt sie keine inhaltliche, sondern rein formale Funktion. Jedes der Unterelemente *Kommentar*, *Grundelement der Rechtsnorm*, *Artikel* und *Begriff* ist null bis beliebig oft im *KommentarModell* enthalten. Nachfolgend werden die einzelnen Bestandteile ausführlich dargestellt, um ihre Funktionen und Beziehungen zu verdeutlichen.

Grundelement der Rechtsnorm: Hier wird der Teil der Rechtsvorschrift genannt, der vom Kommentar beschrieben wird. Es handelt sich hierbei jeweils um einen ausgewähl-

ten Begriff, der als elementarer Bestandteil des zugrundeliegenden Gesetzestextes angesehen wird. Für die DSGVO kann das beispielsweise „Natürliche Person“, „Personenbezogene Daten“ oder auch „Einwilligung“ sein.

Artikel: Gesetzesartikel stehen zwangsläufig in Zusammenhang mit Rechtsnormen. Sei es zum Begründen bestimmter Sachverhalte, als Beleg bei Zitate oder als weiterleitender Verweis zu verwandten Gesetzesstellen sowie zum Nachlesen. Zu diesen vielseitigen Zwecken kann auch hier ein Artikel hinzugefügt werden. Er wird als eigenständiges Element angelegt, um ihn bei mehrfachem Gebrauch wiederverwenden zu können sowie einen späteren Zugriff beziehungsweise eine Abfrage zu erleichtern. Darüber hinaus kann ein Artikel in dem hier verwendeten Sinne aber auch ein Gesetzeskommentar wie beispielsweise aus der Kommentarsammlung von Wolff/ Brink [26] oder ein Erwägungsgrund der DSGVO sein.

Begriff: Kommt in der neu formulierten Erläuterung ein Begriff vor, welcher aufgrund seines komplexen Hintergrunds einer gesonderten Erläuterung bedarf, die nicht in den Kommentar selbst eingebunden werden kann, wird dieser hier angelegt. Dabei enthält das erzeugte Objekt sowohl den Begriff selbst als auch dessen Erläuterung.

Verweise: Ein Kommentar kann innerhalb seiner Erläuterung Bezug auf andere Grundelemente der Rechtsnorm nehmen oder es werden Begriffe verwendet, die aufgrund des Umfangs zu diesem Zeitpunkt nicht in den Kommentar eingebunden werden können. Des Weiteren kann eine Verlinkung zu einem Rechtsartikel hergestellt werden wollen, der in der Erläuterung lediglich als Referenz in Erscheinung treten soll. Diese Verknüpfungen können mittels des Elements „Verweise“ in einen Kommentar hinzugefügt werden.

Kommentar: Beim Kommentar handelt es sich um das Kernelement des Kommentarmodells. Er kann durch alle anderen Elemente des Modells ergänzt werden und enthält somit genau jene Aspekte, die eine aussagekräftige Annotation beinhalten müsste. Verdeutlicht sei noch einmal, dass ein Kommentar somit nicht nur eine Erläuterung ist, sondern ein Konstrukt aus mehreren Bestandteilen.
Verpflichtend enthält er zum einen das Attribut „Erläuterung“. Es erläutert das eindeutig zugeordnete „Grundelement der Rechtsnorm“ und ist das inhaltliche Kernelemt des Kommentars. In der Erläuterung werden die gesamte Beschreibung sowie die zu beachtenden Hinweise des zugeordneten Grundelements dargelegt. Zum anderen wird jedem Kommentar eine eindeutige „Ident“ zugeordnet. Durch sie ist jede spätere Instanz eindeutig zu identifizieren. Die weiteren Elemente des Modells dienen der ausführlicheren Darstellung und anschaulichen Nachverfolgung der Erläuterung. Beispielsweise wird zum Zweck der Rückverfolgbarkeit jeder Kommentar mit mindestens einem zugrundeliegenden DSGVO-Artikel versehen. So weiß ein Softwareentwickler, der mit den Annotationen arbeitet, wo er bei Bedarf in der DSGVO nachlesen oder sich weiterführende Informationen beschaffen kann. Unter „Verweise“ sammeln sich alle verknüpften Begriffe, Artikel oder Grundelemente der Rechtsnorm, die in relevantem Bezug zu den Inhalten der Erläuterung stehen.

5.2. Instanzmodell

Um das entwickelte Kommentarmodell nun auch praktisch verwenden zu können, muss es inhaltlich gefüllt werden. Erreicht wird dies, indem aus dem Metamodell eine Modellinstanz erzeugt wird. Gegenstand dieser Instanziierung kann grundsätzlich jeder Gesetzestext sein, wobei sie im Kontext dieser Arbeit konkret auf die DSGVO bezogen wird. Darüber hinaus wird die Auswahl relevanter Aspekte bereits hier auf die Zielgruppe „Softwareentwickler" zugeschnitten. Ausgangspunkt der Instanziierung bildet das DSGVO-Modell von Boltz et al. (unv.). Da Boltz et al. das Modell im Rahmen der Zusammenarbeit von Softwareentwicklern und Rechtsexperten entwickelt haben, wird angenommen, dass die Klassen des DSGVO-Modells eben jene relevanten Grundelemente der DSGVO widerspiegeln, die auch für den Softwareentwickler von Bedeutung sind. Aus diesem Grund werden sie als *Grundelement der Rechtsnorm* für das Kommentarmodell abgeleitet.

Zu jedem dieser Grundelemente wird ein vollständiger Annotations-Kommentar erstellt. Die Kommentarerstellung folgt den in Kapitel 4 entwickelten Ansätzen zum systematischen Kommentieren, kann nun aber kontextbezogen umgesetzt werden. Als inhaltliche Quellen der Informationszusammenstellung dienen neben der DSGVO in deutscher Sprache, die Kommentare von Wolff/ Brink aus *Datenschutzrecht: DS-GVO, BDSG, Grundlagen, bereichsspezifischer Datenschutz - Kommentar* in der Online-Fassung [25][1] sowie die Erwägungsgründe der DSGVO.

Im Folgenden wird eine solche Kommentar-Instanz beispielhaft am Grundelement „Natürliche Person" der DSGVO veranschaulicht und das Zustandekommen prägnant dargelegt. Zum Vergleich sind in Abbildung 5.2 Ausschnitte der Ecore-Instanz zu sehen.

Grundelement der Rechtsnorm: *Natürliche Person*

Die zugewiesene „Ident" ist prinzipiell ein beliebig zugeteilter Double. Sie wurde hier allerdings zur besseren Übersicht aufsteigend vergeben. Dabei wird bei Oberelementen die Ziffer vor dem Komma und bei Unterelementen die Ziffer nach dem Komma aufsteigend fortgeführt.

Ident: *1.0*

Informationen über Begriffsbestimmungen der *natürlichen Person* und damit Erläuterungen, wer oder was unter dieser zu verstehen ist, finden sich in Art. 4 Nr.1 wieder sowie im Kommentar Art. 4 Rn. 5 von Wolff/ Brink [25]. Aus diesen beiden Quellen werden die inhaltlich relevanten Aspekte zur natürlichen Person im Sinne der DSGVO herausgearbeitet und so weit zielgruppenspezifisch reduziert, dass sie in einer neuen Beschreibung zusammengefasst werden können. So wurde folgende Erläuterung formuliert:

Erläuterung: *Die „Natürliche Person" ist eine lebende und von der juristischen Person abzugrenzende Person. Im Rahmen der DSGVO ist eine natürliche Person stets in ihrer identifizierbaren oder identifizierten Ausprägung zu verstehen. Sie wird auch als betroffene Person bezeichnet. Die personenbezogenen Daten, die sich auf die identifizierbare/ -zierte natürliche Person beziehen, fallen unter den Anwendungskontext der DSGVO und dürfen nur entsprechend der Bestimmungen verwendet werden.*

[1] Wird auf einen solchen Kommentar referenziert, wird dies mit „Komm." eingeleitet

Darüber hinaus werden die beiden Referenzen der Quellen als „Artikel zur Rückverfolgbarkeit“ im Kommentar festgehalten, da es sich hierbei um die Hauptinformationsquellen handelt.

Artikel zur Rückverfolgbarkeit: *Art. 4 Nr. 1; Komm.: Art. 4 Rn. 5*

Des Weiteren treten in der eigens formulierten Erläuterung nun möglicherweise juristische Begriffe auf, die einer Erklärung bedürfen. Für sie bietet sich innerhalb der Erläuterung jedoch unzureichend Raum, weshalb sie den Vermerk als „Verknüpfte Begriffe“ erhalten. Durch ihre übergeordnete Deklaration als „Begriff“, erhalten sie eine Definition und mindestens einen Referenzartikel. Im Gegensatz zum Konzept zur systematischen Kommentierung stehen diese Begriffe im Instanzmodell, wie bereits erläutert, nicht in einem Glossar.

Da in der Kommentar-Erläuterung keine weiteren Artikel referenziert werden und die „Natürliche Person“ auf kein anderes Grundelement Bezug nimmt, sind die weiteren Verknüpfungen leer. Anders wäre dies beispielsweise beim „Dritten“. Dieser kann eine natürliche Person sein, weshalb auf sie verwiesen wird.

Verweise:

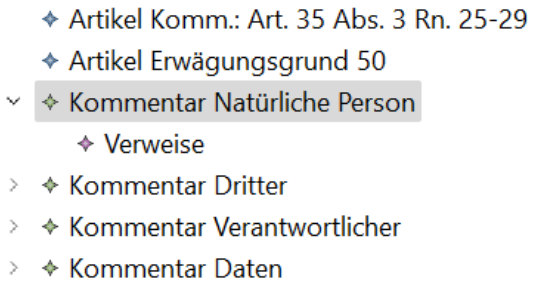
Verknüpfte Begriffe:

Identifizierte/-bare Person: Eine natürliche Person, die insbesondere mittels Zuordnung zu einer Kennung direkt oder indirekt identifiziert werden kann. Zur Feststellung müssen alle Mittel berücksichtigt werden, die nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden. Es ist hierbei nicht entscheidend, dass die Daten zur Identifizierung in einer Hand liegen.
Art. 4 Nr.1; Komm.: Art. 4 Rn. 14-21

Juristische Person: Juristische Personen sind keine einzelnen natürlichen Personen, sondern ein Zusammenschluss von mehreren natürlichen oder juristischen Personen. Juristische Personen des Privatrechts (bspw. Stiftung, GmbH) werden nicht ausdrücklich als Betroffene von der DSGVO erfasst. Sie müssen sich aber gleichermaßen an die DSGVO halten.
Komm.: Art. 4 Rn. 5

Betroffene Person: Bei der betroffenen Person handelt es sich um die identifizierte/ identifizierbare natürliche Person, die davor zu schützen ist, dass ihr Persönlichkeitsrecht durch den Umgang mit ihren personenbezogenen Daten beeinträchtigt wird. Sie ist weder Verantwortlicher, noch Dritter und kann Rechte in Bezug auf ihre personenbezogenen Daten geltend machen (Art. 15-18 DSGVO).
Komm.: Art. 4 Rn. 28; Art. 15-18

Verknüpfte Artikel: -
Verknüpftes Grundelement der Rechtsnorm: -



(a)

Artikel Rückverfolgbarkeit	Artikel Art. 4 Nr. 1, Artikel Komm.: Art. 4 Rn. 5
Entity Name	Natürliche Person
Erläuterung	Die natürliche Person ist eine lebende und von der
Grundelement Rechtsnorm2	Grundelement Rechtsnorm Natürliche Person
Id	KL_3nds_9cJ
Ident	1.0

(b)

Abbildung 5.2.: Ausschnitt des Kommentar-Instanzmodells

5.3. Kommentarkatalog

Um die erarbeitete Instanz des Kommentarmodells zur DSGVO in dieser Arbeit darstellen zu können, wurde sie zusätzlich zum Ecore-Modell in tabellarischer Form als Katalog zusammengestellt. Er ist in Tabelle A.1 zu sehen. Darüber hinaus wurden die verknüpften Begriffe mitsamt Erläuterung und Artikel - wie in 4 vorgeschlagen - in einem Glossar gelistet. Diese Trennung dient lediglich der Anschaulichkeit. Im Kommentarmodell sind die verknüpften Begriffe nicht vom Kommentar getrennt. Abgebildet ist das Glossar in Abbildung A.2.

5.4. Begründung der Auswahl berücksichtigter Artikel und Auslegungen für den Kommentarkatalog

Grundsätzlich könnte jeder Kommentar noch deutlich ausführlicher ausfallen. Nicht nur durch das Hinzufügen der Auslegungsmethodik wäre dies der Fall, sondern durch den Einbezug weiterer DSGVO-Artikel, Gesetzeskommentare oder Erwägungsgründe. Dies hätte den Vorteil, dass ein überaus umfangreiches Bild des einzelnen Gesetzesgegenstandes erreicht werden würde. Doch da die Kommentare auf den spezifischen Anwendungszweck der „Annotation an Softwaremodellen“ zugeschnitten sind, müssen sie in der Anzahl und insbesondere der Ausführungslänge beschränkt werden. Denn ab einer gewissen Informationsmenge ist anzunehmen, dass die Kommentare nicht mehr förderlich sind, sondern ein effizientes Arbeit verhindern. Die Anzahl der Kommentare wurde bereits durch die Festlegung, dass die Klassen des DSGVO-Modells die Grundelemente der Rechtsnorm

widerspiegeln, beschränkt. Nun musste noch aus den zugrundeliegenden Quellen eine Auswahl an relevanten Aspekten getroffen werden. Dies geschah mit dem Wissen, keine erschöpfende Kommentar-Ausarbeitung als Endprodukt bieten zu können. Eine Auswahl an Entscheidungen soll hier dargelegt werden.

Von Bedeutung für die Auswahl war, dass die Kommentarinhalte auf die Zielgruppe zugeschnitten sein sollen. Sie müssen so gestaltet sein, dass ein Nutzer zielführend mit ihnen arbeiten kann. Dafür dürfen sie einerseits keinen zu geringen Informationsgehalt aufweisen, andererseits besteht bei einer zu hohen Informationslast das Potential einer Überforderung. Den Kommentaren wird somit die Aufgabe zuteil, einen angemessenen Überblick über den Sachverhalt zu geben. Um diesen Anforderungen zu entsprechen, ist es sinnvoll, die Inhalte bereits auf den späteren Anwendungskontext zu beziehen und irrelevante Bestandteile wegzulassen.

Das Abschlussartefakt dieser Arbeit soll Softwareexperten bei der datenschutzkonformen Entwicklung von Softwaremodellen unterstützen und wird zumindest zu Beginn im Mobility-Bereich eingesetzt werden. Durch diese Festlegung wird der Anwendungsbereich bereits beschränkt und es wird ersichtlich, dass aufgrund des Laienstatus' der Nutzer überwiegend grundlegende Basisinformationen und Erklärungen der DSGVO benötigt werden. So muss beispielsweise primär verdeutlicht werden, für wen die Grundsätze des Datenschutzes und der Verarbeitung personenbezogener Daten gelten und welche Art von Daten in den Geltungsbereich fallen. Darüber hinaus können bereits bestimmte Kapitel der DSGVO als sekundär herausgefiltert werden. In diesem Schritt wurden die von Torre et al. vorgeschlagenen Exklusionen (vgl. Kapitel 3.1) als Anhaltspunkt für die hier vorgenommene Auswahl genommen. So können beispielsweise Kapitel, die sich auf spezifische Informationen zur Errichtung von Aufsichtsbehörden oder auf Sanktionsbestimmungen beziehen exkludiert werden. Für den Softwareentwickler scheint es in erster Linie nur von Bedeutung, zu wissen, dass es eine Aufsichtsbehörde gibt und wann sie für ihn beziehungsweise für Prozesse innerhalb der Software relevant ist - nicht wie und warum sie errichtet wird. Ebenso ist nur das Bewusstsein darüber, dass bei Verstößen Sanktionen drohen, relevant - nicht die Sanktionen im Einzelnen. Und dennoch ist dem Softwareentwickler die Wichtigkeit der Einhaltung ersichtlich. Darüber hinaus wurde auf die Ausführung von länderspezifischen Regelungen verzichtet. Da die DSGVO im Zentrum dieser Arbeit steht und das BDSG aus dieser hervorgeht, wurde auf eine Verknüpfung zu korrelierenden Rechtsnormen aufgrund der erhöhten Komplexität verzichtet.

Eine Frage tut sich auf: ist ein Nutzer, wenn die DSGVO für ihn bisher vergleichsweise unbekannt war, an Informationen darüber interessiert, wie eine Bestimmung zustande gekommen ist? Aus der Theorie heraus kann diese Frage nicht abschließend entschieden werden. Doch soll die hier getroffene Entscheidung, dass darauf verzichtet werden kann, kurz begründet werden. Wird ein rein praktischer und effizienter Standpunkt eingenommen, so scheint der Softwareentwickler nicht wissen zu müssen, wer aus welchen Gründen eine Bestimmung festgelegt hat. Er muss nur das Ergebnis in seiner Software berücksichtigen. Entscheidend ist also, was er datenschutzrechtlich umsetzen oder nicht umsetzen darf. An dieser Stelle wird ein mögliches Problem erkennbar, welches in der Evaluation noch einmal ausführlicher aufgegriffen wird. Denn das Weglassen von Begründungen kann ebenfalls zu Herausforderungen führen, wenn Spezial- oder Randfälle behandelt werden müssen. In solchen Fällen wird schließlich ein komplexeres Verständ-

nis des Rechtsgegenstandes benötigt, da nicht mehr nur einem einzelnen Muster gefolgt werden kann. Andererseits soll eine ausführliche Annotation den Nutzer auch nicht dazu verleiten, rechtlich schwierige Fragen alleine zu entscheiden. An dieser Stelle sollte auf die Zusammenarbeit mit einem Juristen zurückgegriffen werden.

6. Automatisiertes Annotieren der Kommentare

Durch die Konzeption des Kommentarmodells sowie der Ausformulierung der Kommentare kann nun der Annotationsmechanismus entwickelt werden. Letztliches Ziel der automatisierten Annotation ist es, eine Instanz des DSGVO-Modells zu laden und jedes Element dieser Instanz mit einem entsprechenden Kommentar zu versehen. Dies geschieht in mehreren Schritten. Zuerst wird ein allgemeines Annotationsmodell konstruiert, welches die strukturelle Grundlage bietet, jeweils ein Element des Kommentarmodells und des DSGVO-Modells miteinander zu verknüpfen und in einer Liste abzuspeichern. Mithilfe dieses Modells kann anschließend ein Annotationsmechanismus geschrieben werden, welcher den Kommentar zu einem bestimmten DSGVO-Element findet und beide gemeinsam als Paar abspeichert. Diese Annotation muss so konzipiert sein, dass sie sich im Späteren auf eine beliebige DSGVO-Instanz beziehen kann und weiterhin die korrekten Annotationen zuordnet sowie ausgibt.

6.1. Annotationsmodell

Die grundlegende Idee hinter dem Annotationsmodell ist es, ein beliebiges Rechtsmodell[1] zu nehmen und jedem seiner Elemente genau einen Kommentar des zugehörigen Kommentarmodells zuzuordnen. Im späteren Anwendungsgebrauch soll es sich bei dem Rechtsmodell schließlich um eine Instanz handeln, welche aus einem konkreten Softwareprodukt abgeleitet wurde. Eine solche Anwendung wird in der Evaluation einer Fallinstanz in Kapitel 7 am Beispiel der Travel Planner Application [3] ausgewertet.

Um diese Idee umzusetzen, wird im Annotationsmodell das Metamodell der DSGVO mit dem Kommentarmodell verknüpft. Das Annotationsmodell stellt erst einmal noch keine aktive Annotierung dar, sondern bietet die strukturelle Voraussetzung dafür. Es besteht zum einen aus der „Annotation“ und zum anderen aus der „Annotationsliste“, welche keine bis viele Annotationen enthalten kann. Eine einzelne Annotation hingegen beinhaltet einen Kommentar vom Typ *Kommentar* des Kommentarmodells sowie das dazugehörige Element des Rechtsmodells vom Typ *AbstractGDPRElement*. Letzteres ist eine abstrakte Klasse, wodurch je nach Zuordnung jede der Unterklassen ausgegeben werden kann. Das Modell ist in Abbildung 6.1 illustriert.

[1] Im Folgenden wird immer spezifisch auf das Modell der DSGVO Bezug genommen, auch wenn theoretisch jedes Rechtsmodell verwendet werden kann.

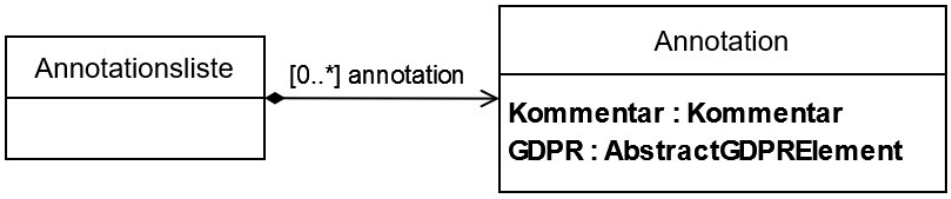


Abbildung 6.1.: Annotationsmodell

6.2. Annotationsmechanismus

Der nun folgende Annotationsmechanismus nutzt diese Struktur des Annotationsmodells, um das Paar-Objekt zu erstellen und es anschließend in der Liste abzuspeichern. Es bleibt somit noch die Aufgabe, die Verlinkung der beiden Elemente zu implementieren. Zu diesem Zweck soll ein Annotationsvorgang erstellt werden, der jedem *AbstractGDPRElement* einen zugehörigen Kommentar zuordnet, diese in einer Liste von Annotationen sammelt und letztere abschließend speichert. Der Vorgang muss soweit abstrahiert sein, dass er auf verschiedenste Instanzen des DSGVO-Modells anwendbar ist.

6.2.1. Struktur

Hierzu wird ein Java-Projekt, welches mit *DSGVOLinkKommentar* benannt wurde, erstellt. Auf die bereits bestehenden Modelle wird referenziert, sowie der von EMF automatisch zu den Modellen generierte Programmcode genutzt. Im ersten Schritt bedeutet dies, dass die drei Modelle - DSGVO-Modell, Kommentarmodell und Annotationsmodell - in die „Dependencies“ des Java-Projekts *DSGVOLinkKommentar* eingetragen werden, um Zugriff auf die Ecore-Projekte zu erhalten. Des Weiteren werden jeweils das Instanzmodell des Kommentarmodells sowie des DSGVO-Modells in einem Projektordner - hier „modelle“ - abgelegt. Die Instanz des DSGVO-Modells kann jederzeit durch eine andere Instanz ersetzt werden und ist somit für jedes Softwareprojekt einsetzbar. Wird eine Veränderung an Kommentaren vorgenommen, so muss auch diese Datei neu abgelegt werden. Durch die Ablage der Instanzen kann nun auf die Kommentare einerseits und die DSGVO-Instanzelemente andererseits zugegriffen werden. Zu sehen sind die beiden abgelegten Instanzen in 6.2 als *.gdpr* und *.kommentarmodell*.

6.2.2. Implementierung

Es werden zwei Java-Klassen benötigt, um den Annotationsmechanismus und damit die Annotationsliste zu erzeugen. Sie basieren unter anderem auf der Verwendung von EMF-generiertem Code, welcher insbesondere für die Instanziierung der Modelle verwendet wird. Die Klasse *Annotierer* beinhaltet die Methoden zum Laden und Initialisieren der Instanzmodelle. Dabei werden jeweils die Oberelemente der Modelle *LegalAssessment-*

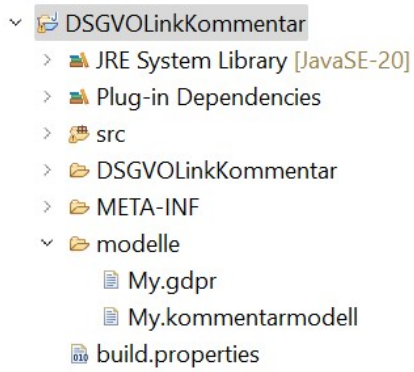


Abbildung 6.2.: Projektordner

Facts und *KommentarModell*, welche die einzelnen Bestandteile ihres jeweiligen Modells enthalten, zurückgegeben.

Neben den beiden Methoden zum Laden der aktuellen Modelle enthält die Klasse eine Hilfsmethode, welche den Namen der Modelldatei bei Eingabe des entsprechenden Dateityps zurückgibt. Dies setzt zwar einerseits voraus, dass die im Ordner „modelle“ abgelegten Dateien ausschließlich vom Typ *.gdpr* sowie *.kommentarmodell* sind und jeder der beiden Dateitypen nur genau einmal vorkommt. Andererseits muss dadurch der vollständige Dateiname nicht in den Lademethoden festgeschrieben werden, wodurch eine Änderung des Programmcodes innerhalb der Lademethode beim Austausch der Dateien nicht notwendig ist.

In der *Main-Klasse* werden nun die Elemente und Kommentare der beiden Modelle verglichen, einander zugeordnet und die Paare in die Annotationsliste eingefügt. Hierzu werden zu Beginn die Modelle mittels der Methoden der *Annotierer-Klasse* geladen sowie ein Annotationsliste[n]-Objekt erzeugt. Die Zuordnung der Elemente zu den passenden Kommentaren erfolgt über einen *instanceOf*-Abfrage der Typklassen. Eine Typklasse ist dabei eine der Klassen aus dem in Abschnitt 2.5 vorgestellten DSGVO-Modell. Für jedes Element der DSGVO-Instanz werden die möglichen Superklassen durchlaufen und der entsprechende Subtyp gesucht. Beispielsweise wird ein Element vom Typ „LegalBasis“ darauf getestet, ob es den Typ „PerformanceOfContract“, „Consent“, „ExerciseOfPublicAuthority“ oder nur den allgemeinen Typ „LegalBasis“ aufweist. Ein Ausschnitt dieser Abfrage ist in Listing 6.1 zu sehen. Wurde der entsprechende Typ festgestellt, so werden die Parameter an eine Hilfsmethode zum Setzen des Annotationseintrages übergeben. Zu den Parametern gehören die Typklasse als String, das DSGVO-Element, die Liste der Kommentare der Kommentar-Instanz sowie die bisherige Annotationsliste. Mittels der Hilfsmethode wird dann der zugehörige Kommentar aus der Kommentarliste herausgesucht und mit dem übergebenen DSGVO-Element zu einer Annotation zusammengestellt. Dieses wird schließlich der Annotationsliste hinzugefügt.

```
public class Main {
    public static void main(String[] args){
        ...
        for (LegalBasis rechtsgrundlage : gdpr.getLegalBasis()) {
            if (rechtsgrundlage instanceof PerformanceOfContract) {
                setAnnotationEintrag("Vertragserfuellung", rechtsgrundlage, eintragListe,
    annotationsliste);
            } else if (rechtsgrundlage instanceof Consent) {
                setAnnotationEintrag("Einwilligung", rechtsgrundlage, eintragListe,
    annotationsliste);
            } else if (rechtsgrundlage instanceof ExerciseOfPublicAuthority) {
                setAnnotationEintrag("Ausuebung der oeffentlichen Gewalt/ Behoerde",
    rechtsgrundlage, eintragListe, annotationsliste);
            } else if (rechtsgrundlage instanceof LegalBasis) {
                setAnnotationEintrag( "Rechtsgrundlage", rechtsgrundlage, eintragListe,
    annotationsliste);
            }
        }
 ...
}
```

Listing 6.1: Beispielausschnitt der Typabfrage und Übergabe der Parameter an die Eintrag-Methode

Da die Modellierung des Ecore-DSGVO-Modells ermöglicht, dass ein Element ausschließlich eine Superklasse repräsentiert, zum Beispiel wenn ein Element vom Typ *Processing* ist, erfolgt erst die Subtyp-Abfrage und im Anschluss die Typabfrage auf den Supertyp. So wird umgangen, dass die Elemente direkt dem Supertyp zugeordnet werden. Des Weiteren stellt *Proof* eine Ausnahme dar. Dieser Typ besitzt keine Superklasse, weshalb der Eintrag bei einem solchen Element ohne weitere Typabfragen direkt zugeordnet wird.

Im Anschluss an die Zuordnung aller DSGVO-Elemente zu einem Kommentar wird die vollständige Annotationsliste als XMI-Datei abgespeichert. Wie eine solche Liste beispielhaft aussehen kann, ist in Listing 6.2 nachzuvollziehen. Allerdings werden in dieser Liste nicht die vollständigen Kommentare mit allen ihren Bestandteilen ausgegeben, sondern lediglich die Referenzen auf den Kommentar sowie auf das DSGVO-Element. Das Ausgabeformat der Liste muss für die Praxisanwendung dementsprechend überarbeitet werden. Dieser Nachteil wird in Kapitel 8 zu zukünftigen Arbeitsschritten noch einmal aufgegriffen.

```
<annotation>
    <Kommentar href="modelle/My.kommentarmodell#Vertragserfuellung"/>
    <GDPR xsi:type="GDPR:PerformanceOfContract" href="modelle/My.gdpr#
    _g5XTmWgvEe6fTZX5P0PPwA"/>
  </annotation>
  <annotation>
    <Kommentar href="modelle/My.kommentarmodell#Rechtsgrundlage"/>
    <GDPR xsi:type="GDPR:LegalBasis" href="modelle/My.gdpr#_m3eauHcrEe69Lv-Z5rOP2g"/>
  </annotation>
  <annotation>
```

Listing 6.2: Ausschnitt aus einer erzeugten Annotationsliste mit beispielhaftem DSGVO-Instanzmodell

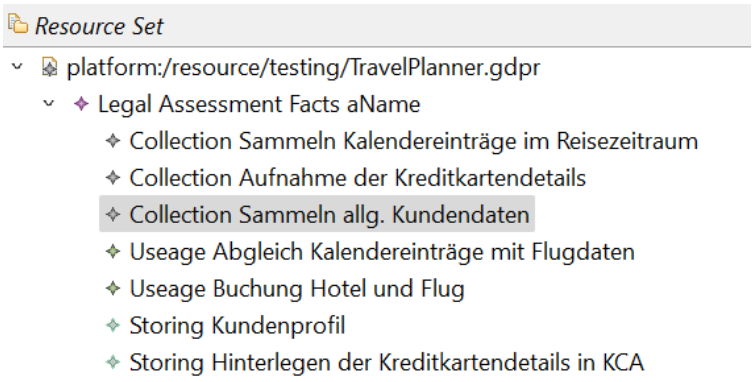
7. Evaluation

Ziel der Evaluation soll es sein, den entwickelten Annotationsmechanismus auszuwerten. Dafür soll die Funktionsfähigkeit, Vollständigkeit und Korrektheit der Annotationsliste überprüft werden. Des Weiteren stellt sich mit Blick auf den entwickelten Ansatz einerseits die Frage, ob er auf verschiedenste DSGVO-Instanzen allgemeingültig anwendbar ist. Gleichzeitig aber auch, ob er den Anforderungen des spezifischen Anwendungsbereichs der Softwareentwicklung gerecht wird. Auf eine Aussage über die inhaltliche Nutzbarkeit sowie Anwendbarkeit der Kommentare in der Praxis muss in dieser Evaluation verzichtet werden. Für die dafür notwendige Nutzerstudie waren die Ressourcen nicht ausreichend, weshalb sie nicht angefertigt werden konnten.

Die Evaluation dient somit ebenfalls dem Aufdecken noch fehlender Aspekte und Schwierigkeiten beziehungsweise Probleme, die in zukünftige Arbeit aufgenommen werden sollten. Unterstützt wird die Evaluation im ersten Teil durch eine Instanz einer Fallstudie. Bei dieser handelt es sich um ein Software-Praxisbeispiel, welches als DSGVO-Instanz modelliert wird. Anschließend wird darauf der Annotationsmechanismus angewendet. Die resultierenden Ergebnisse können schließlich der Evaluation unterzogen werden.

7.1. Instanz einer Fallstudie - Travel Planner Application

Zur Evaluation des entwickelten Annotationsmechanismus' wird eine Instanz einer Fallstudie erstellt. Bei der gewählten Fallstudie handelt es sich um die Travel Planner Application (*TPA*) vom Institut für Software und Systems Engineering der Universität Augsburg (ISSE) [3]. Sie dient als Grundlage zur Modellierung der Test-Modellinstanz. Aus den beteiligten Parteien, Beziehungen und Workflows der TPA wird eine entsprechende DSGVO-Instanz erstellt, indem ebendiese Einzelbestandteile auf die entsprechenden Klassen des DSGVO-Modells projiziert werden. Beispielsweise stellt ein Kunde der TPA eine „natürliche Person" dar, eine Airline bildet einen „Dritten" ab und das Hinterlegen von Kreditkartendetails ist eine Verarbeitung in Form der „Speicherung". Diese Instanzbildung ist in Abbildung 7.1 a) beispielhaft dargestellt. Abbildung 7.1 b) zeigt hingegen detailliert die einzelnen Bestandteile eines Instanzelements. Die Bestandteile sind jene, die im DSGVO-Metamodell definiert wurden. Anschließend wird diese Instanz als Eingabe für den Annotationsvorgang genutzt und das Ergebnis, also die gespeicherte Annotationsliste, ausgewertet.



(a)

Property	Value
Entity Name	Sammeln allg. Kundendaten
Following Processing	Storing Kundenprofil
Id	_bJa4WgvEe6fTZX5P0PPwA
Input Data	Personal Data Kundendaten
On The Basis Of	Consent Einwilligung in die App-Bedingungen
Purpose	Purpose Reiseauskunft

(b)

Abbildung 7.1.: Ausschnitt des Instanzmodells der TPA

7.1.1. Auswertung der Travel Planner-Instanz nach Goldstandard: Accuracy, Precision, Recall

Listing 7.1 zeigt einen Ausschnitt der Annotationsliste, die aus den Instanzen des Kommentarmodells und der *Travel Planner Application* generiert wurde. Sie soll als Beispiel dienen, um der Evaluation anschaulich folgen zu können. Es ist zu sehen, dass zum einen eine Annotationsliste aus mehreren Annotationen besteht. Zum anderen enthält jede Annotation jeweils genau eine Referenz auf einen Kommentareintrag sowie eine Referenz auf ein DSGVO-Element. Dies gilt für die gesamte Liste. Da eine einzelne Annotation immer aus eben diesen beiden Elementen bestehen muss, ist die Bedingung für eine korrekte Annotation erfüllt. Alle Paare wurden aus struktureller Sicht korrekt gebildet.

Im nächsten Schritt soll die Liste auf Vollständigkeit geprüft werden. Um diese Anforderung zu erfüllen, muss jedes Element der TPA-Instanz genau einmal in der Annotationsliste vorkommen. Somit muss es genau so viele Annotationseinträge in der Liste geben wie Elemente in der TPA-Instanz sind. Die Instanz beinhaltet in diesem konstruierten Beispiel 38 Elemente und auch die Liste erfasst genau 38 Annotationen. Die Vollständigkeit ist somit in dieser Hinsicht erfüllt.

Des Weiteren ist die inhaltliche Korrektheit der Paare durch einen Vergleich der Bezeichnungen der „href“-Referenz des Kommentareintrags und dem „type“ des DSGVO-Elements zu erkennen[1] Auch diese Korrektheit ist erfüllt.

[1]Unter Beachtung der unterschiedlich sprachigen Modelle.

```
...
  <annotation>
    <Kommentar href="modelle/My.kommentarmodell#Daten"/>
    <GDPR xsi:type="GDPR:Data" href="modelle/TravelPlanner.gdpr#_mjFxtWguEe6fTZX5P0PPwA"/>
  </annotation>
  <annotation>
    <Kommentar href="modelle/My.kommentarmodell#Natuerliche Person"/>
    <GDPR xsi:type="GDPR:NaturalPerson" href="modelle/TravelPlanner.gdpr#
    _qne0LGguEe6fTZX5P0PPwA"/>
  </annotation>
  <annotation>
    <Kommentar href="modelle/My.kommentarmodell#Verantwortlicher"/>
    <GDPR xsi:type="GDPR:Controller" href="modelle/TravelPlanner.gdpr#
    _tQoArWguEe6fTZX5P0PPwA"/>
  </annotation>
  <annotation>
    <Kommentar href="modelle/My.kommentarmodell#Nachweis"/>
    <GDPR xsi:type="GDPR:Proof" href="modelle/TravelPlanner.gdpr#_EL2mQGgvEe6fTZX5P0PPwA"/>
  </annotation>
  <annotation>
    <Kommentar href="modelle/My.kommentarmodell#Nachweis"/>
    <GDPR xsi:type="GDPR:Proof" href="modelle/TravelPlanner.gdpr#_E-ouEGgvEe6fTZX5P0PPwA"/>
  </annotation>
  <annotation>
    <Kommentar href="modelle/My.kommentarmodell#Dritter"/>
    <GDPR xsi:type="GDPR:ThirdParty" href="modelle/TravelPlanner.gdpr#
    _zYv1kWguEe6fTZX5P0PPwA"/>
  </annotation>
  ...
```

Listing 7.1: Ausschnitt aus der generierten Annotationsliste mit der Travel Planner Application als DSGVO-Instanzmodell

Zur Auswertung können darüber hinaus die statistischen Gütekriterien *Accuracy*, *Precision* und *Recall* angeführt werden. Sie bestätigen die obige Auswertung der Korrektheit.

Accuracy:

Korrektklassifikationsrate:
$P(richtigZugeordnet|allePaare) = \frac{38}{38} = 1.0$
Falschklassifikationsrate:
$P(falschZugeordnet|allePaare) = \frac{0}{38} = 0.0$
Zusammenhang:
$Korrektklassifikationsrate + Falschklassifikationsrate = 1.0$

Precision:
$P(korrektePaare|gewhltePaare) = \frac{38}{38} = 1.0$
Recall:
$P(korrektePaare|relevantePaare) = \frac{38}{38} = 1.0$

7.1.2. Inhaltliche Präzision

In Hinblick auf die inhaltliche Genauigkeit der Annotation sind gegebenenfalls Verbesserungen möglich. Im Instanzmodell der DSGVO ist es möglich, Supertypen zu instanziieren, auch wenn dem Element ein konkreter Subtyp zuzuordnen wäre. Beispielsweise kann für eine Verarbeitung im Rahmen der „Nutzung“ auch lediglich „Verarbeitung“ angegeben werden. Dadurch wird eine spezifische Beschreibung durch einen genaueren Kommentar verhindert. Zusätzlich erhält der Nutzer nicht alle relevanten Informationen, die für seine Arbeit eigentlich nötig wären. Eine solch allgemeinere Annotationsausgabe ist nur dann von Vorteil, wenn der Nutzer aufgrund fehlenden Wissens das DSGVO-Element tatsächlich nicht genauer zuordnen kann. So wird zumindest eine grobe Beschreibung des zugrundeliegenden Rechtsgegenstandes annotiert, was zielführender ist, als das Element wegzulassen.

Darüber hinaus kann die Nutzung von Supertypen in der Instanziierung auch vorteilhaft sein, da das zugrundeliegende DSGVO-Modell nicht erschöpfend ist. Aufgrund der in Abschnitt 5.4 begründeten Reduktion werden nicht alle Sachverhalte der DSGVO erfasst, weshalb es sinnvoll sein kann, gewisse Verallgemeinerungen zuzulassen. Hier steht somit ein potentiell hoher Grad ungewollter Ungenauigkeit einer möglicherweise sinnvollen Verallgemeinerung gegenüber.

Ein weiterer Aspekt im Bereich der Präzision bezieht sich auf die Möglichkeit, im DSGVO-Instanzmodell Sachverhalte instanziieren zu können, die sich nicht auf personenbezogene Daten oder Verarbeitungen derselben beziehen. Sie fallen somit gar nicht in den Gegenstandsbereich der DSGVO, werden aber dennoch annotiert. Dies scheint erst einmal nicht zweckerfüllend. Zielführend kann es allerdings dennoch sein, um ein Modell und die zugehörigen Prozesse ganzheitlich darstellen zu können. Wäre es lediglich möglich, die DSGVO relevanten Aspekte darzustellen, würde womöglich der Zusammenhang des zugrundeliegenden Instanzmodells nicht vollständig ersichtlich werden. Es bestünde das Risiko, dass einzelne Verknüpfungen aus dem Blickfeld geraten, obwohl sie womöglich doch einen bis dato unbekannten datenschutzrechtlich relevanten Aspekt enthalten.

7.2. Nutzbarkeit und Funktionalität

Um die Anwendbarkeit und effiziente Nutzung der Kommentare in der Praxis evaluieren zu können, bedarf es Tests und Nutzerstudien mit der Zielgruppe. Solche Studien wurden im Rahmen der Bachelorarbeit nicht angefertigt. In Kapitel 8.1 zu den zukünftigen Arbeiten wird auf die ausstehende Evaluation näher eingegangen.

Eine Aussagen über die Nutzbarkeit und Funktionalität der Annotationen kann auf Grundlage des Ausgabeformats der Annotationsliste dennoch getätigt werden. In dieser werden die Kommentare sowie DSGVO-Elemente lediglich mittels Referenzen abgespeichert. Es ist davon auszugehen, dass ein Softwareentwickler mit diesen Referenzen allerdings nicht sinnvoll arbeiten kann. Er benötigt die vollständige Ausgabe des Kommentars - aufgegliedert in die einzelnen Bestandteile. Nur so kann er auf einfachem Wege die Erläuterungen in seine Softwareentwicklung einbeziehen. Dieser Aspekt wird in Kapitel 8.2 zur zukünftigen Arbeit erneut aufgegriffen.

Im Gegensatz zur fehlenden praktischen Auswertung der Kommentare, wurde das Konzept zur systematischen Kommentierung bestehenden Rechts gewissermaßen umfangreich bei der Entwicklung des Kommentarkatalogs getestet und war in diesem Einsatz erfolgreich umsetzbar. Noch ausstehend ist hier die Validierung, ob das Konzept, wie gefordert, auch auf andere Rechtsvorschriften als die DSGVO anwendbar ist. Da es sich um ein strukturelles Konzept handelt, ist von einer Übertragbarkeit auszugehen.

7.2.1. Umgang mit Änderungen

Das entwickelte Annotationsmodell und die zugehörige Erstellung der Liste sind im Falle von Änderungen einfach zu handhaben. Vorausgesetzt, die Instanzen selbst wurden korrekt erstellt. Wurden Veränderungen an der bestehenden Modellinstanz vorgenommen oder eine vollständig neue Modellinstanz des DSGVO-Modells erstellt, so muss die Instanzdatei erneut im entsprechenden „modelle“-Ordner abgelegt werden. Zu beachten ist dabei, dass sich immer nur genau eine Instanz des DSGVO-Modells bzw. des Kommentarmodells im Ordner befindet. Andernfalls können die beiden Dateien vom Annotationsmechanismus nicht korrekt gefunden und geladen werden.

Eine inhaltliche Änderung der DSGVO-Instanz ist ebenfalls ohne Veränderung des Programmcodes möglich, sofern die Bezeichnungen der Bestandteile des rechtlichen Konzepts nicht verändert oder keine neuen Bestandteile hinzugefügt werden. Da die Abfrage im Annotationsmechanismus auf diesen Bezeichnungen basiert, müsste sie in einem solchen Fall ebenfalls entsprechend geändert werden. Begriffe, Artikel, Erläuterungen und der Kommentar können beliebig verändert oder ergänzt werden. Sie haben keinen Einfluss auf den Programmcode. Voraussetzung dabei ist nur, dass die erstellte Kommentar-Instanz in sich korrekt bleibt. Dies bedeutet, dass es nur genau einen Kommentar für jeden Bestandteil des rechtlichen Konzepts geben darf und muss. Diese Bedingung kann bei der Erstellung der Ecore-Instanz nicht vorgegeben werden. Die Änderung der Kommentarinstanz ist allerdings im späteren Praxisgebrauch nicht regulär vorgesehen. Es handelt sich vielmehr um ein festes Artefakt, welches in regelmäßigen Abständen und in Reaktion auf Rückmeldungen der Nutzer verbessert werden kann. Dahingegen soll das Einfügen neuer DSGVO-Instanzen genau die angestrebte praktische Anwendung des Softwareentwicklers sein.

7.2.2. Bedrohung der Gültigkeit

Der Annotationsmechanismus und die Aussagekraft der verfassten Kommentare wurden bisher nicht von einem Softwareentwickler in der praktischen Anwendung getestet. Aus diesem Grund ist nicht abschließend zu beurteilen, ob die zu Beginn formulierten Anforderungen an die beiden Artefakte erreicht werden. An einer Fallinstanz wurde bereits gezeigt, dass die Annotierung für das spezifische Beispiel korrekt funktioniert. Eine internale Validität ist somit gegeben. Dem gegenüber ist die externe Validität eingeschränkt, da über die tatsächliche Nutzbarkeit dieser Annotierungen infolge fehlender praktischer Erfahrung keine Aussage getätigt werden kann.

Aufgrund der Reduktion der DSGVO auf die hier erstellten Kommentare, kommt es zu einer subjektiven Auswahl der als relevant erachteten Inhalte. Hinzu kommt eine ge-

wisse Interpretation der ausgewählten Rechtsnormen, um sie für den Softwareentwickler verständlicher zu formulieren. Zugleich wurde sowohl die Reduktion als auch die Interpretation nicht von Rechtsexperten vorgenommen. In Summe lässt sich daraus validieren, dass das entwickelte Konzept einerseits umsetzbar ist, jedoch Gültigkeit nur in einem gewissen Rahmen aufweist. Dieser Rahmen bedeutet, dass das Konzept nicht uneingeschränkt verallgemeinerbar ist und stellt. Vielmehr dient es als unterstützendes Werkzeug in der Softwareentwicklung.

8. Zukünftige Arbeit

Die in dieser Arbeit erzielten Ergebnisse stellen einen Teil des übergeordneten Ziels dar, die Zusammenarbeit zwischen Rechts- und Softwareexperten in der Softwareentwicklung zu vereinfachen. Erreicht wird dies im Speziellen durch Annotationen, die dem Softwareentwickler ein höheres inhaltliches Grundverständnis, Bewusstsein und eine Sensibilität für Aspekte der DSGVO vermitteln sollen. Dadurch können eigenständiger als bisher datenschutzkonforme Softwareprodukte entwickelt werden. Um dieses Ziel zu erreichen, fehlen jedoch noch weitere Entwicklungsschritte des Annotationskonzepts.

8.1. Evaluation durch Nutzerstudien

Der zweite Hauptbestandteil weiterführender Arbeit besteht in der umfangreichen Evaluation der Nutzbarkeit der Annotationen. Diese sollte mittels Nutzerstudien durchgeführt werden. Insbesondere sollte der Schwerpunkt auf der inhaltlichen Auswertung der Kommentare liegen. Wie nutzbar, sinnvoll und anwendbar sind die Kommentare der Annotation in der Praxis? Erreichen sie das Ziel, eine selbstständigere Arbeit des Softwareentwicklers zu ermöglichen und vermitteln sie ihm ein Grundverständnis der DSGVO, sodass es ihn bei der Erstellung eines datenschutzkonformen Softwaremodells unterstützt? Zum Ziel der Zusammenarbeit stellt sich die Frage: Erleichtert es tatsächlich die Zusammenarbeit zwischen Rechts- und Softwarebereich? Oder entsteht für den Rechtsexperten letztlich ein größerer Zeitaufwand in der Überprüfung des Modells, weil der Entwickler nun relevante Entscheidungen vollständig ohne juristische Beratung trifft, woraufhin der Rechtsexperte diese ausfindig machen und aufarbeiten muss?

Um die Anwendbarkeit und effiziente Nutzung in der Praxis zu testen, muss mindestens eine Nutzerstudie mit der Zielgruppe „Softwareentwickler“ durchgeführt werden. Nur so kann einerseits ein umfassendes Bild darüber entstehen, ob die Kommentare inhaltlich aussagekräftig, sprachlich für die Zielgruppe zugänglich sowie detailliert genug sind. Und andererseits kann anhand dessen evaluiert werden, ob die Annotationen im Gesamten zielführend dahingehend sind, dass die gegebenen Hinweise vom Softwareentwickler im Softwaremodell erfolgreich verstanden und umgesetzt werden können. Erfolgreich meint in diesem Zusammenhang, dass die gegebenen Hinweise auf Vorschriften, Regelungen etc. wahrgenommen und im Modell nach bestem Können berücksichtigt werden. Und „erfolgreich“ meint weiterhin eine Reduzierung des zeitlichen Aufwands für die Zusammenarbeit mit Juristen.

Es bietet sich an, eine solche Studie in zukünftigen Arbeiten, wenn zugleich das Entwicklungsstadium des Annotationsmechanismus fortgeschritten ist, einzubinden. Insbesondere, wenn die Darstellung der Annotationsliste ausgearbeitet wurde und am Modell direkt an-

notiert wird. So sind die tatsächliche Praxisanwendung und die Funktionalität realistischer und effektiver zu evaluieren.

Ferner ist denkbar, die Studien in regelmäßigen Abständen zu wiederholen, um den Lernprozess der Softwareentwickler zu evaluieren. Sollte sich zeigen, dass sie nach einer gewissen Lernphase ausreichend Expertise entwickelt haben, und die Annotationen somit keinen Mehrwert mehr erzielen, können die Kommentare nachjustiert und der Katalog aus Abschnitt 5.3 erweitert werden. Allerdings muss in diesem Fall berücksichtigt werden, dass es weiterhin Erstbenutzer geben wird, die einen geringeren Erfahrungsstand aufweisen. Der Trade-Off zwischen niedrigerem, aber gleichen Level für alle und höherem, jedoch nicht für alle sinnvoll nutzbaren Level muss in diesem Fall abgewogen werden. Auch hier könnten Nutzerstudien weiterhelfen. Allerdings erscheint der Aufwand sehr hoch.

Des Weiteren wurde der Goldstandard nur an eine konkrete Instanz einer Fallstudie angelegt. Um eine allgemeingültige Aussage über die Präzision treffen zu können, muss die Annotation an weiteren - womöglich auch komplexeren - Fallinstanzen getestet werden.

8.2. Implementierungsverbesserung und Eingabe-/ Ausgabeformat der Annotationsliste

In dieser Arbeit wurde angenommen, dass das Eingabeformat des Annotationsmechanismus' neben der Kommentar-Instanz eine DSGVO-Instanz ist. Dies ist von der praktischen Anwendung in der Arbeit eines Softwareentwicklers allerdings weit entfernt. Es stellt einen erhöhten Zeitaufwand dar, wenn ein Entwickler das Softwaremodell erst einmal in eine DSGVO-Instanz übersetzen muss. Insbesondere setzt es aber Wissen über das Annotationsmodell sowie die DSGVO voraus, welches der Entwickler zu diesem Zeitpunkt noch nicht besitzt und über das Annotationsmodell auch nicht zwangsläufig besitzen soll. Für das Wissen über die DSGVO sollen schließlich die Annotationen dienen. Aus diesem Grund ist Ziel zukünftiger Arbeit, die Umwandlung eines Softwaremodells in eine DSGVO-Instanz zu entwickeln sowie umgekehrt. Durch eine solche Transformation kann die passende Annotation zu einem DSGVO-Instanzelement ermittelt werden und diese wird dann durch die Rück-Transformation auf das zugehörige Softwareelement oder die Relation übertragen. Damit wird zusätzlicher Aufwand für den Entwickler vermieden und Fehler, die bei händischer Umwandlung entstehen könnten, werden vermieden. Darüber hinaus benötigt der Entwickler kein Hintergrundwissen über die Funktionsweise des Annotationsmechanismus'.

Ebenso bestehen Verbesserungsmöglichkeiten bezüglich der Ausgabe-Visualisierung. Das aktuelle Ausgabeformat der Annotationsliste beinhaltet Referenzen auf die entsprechenden Kommentare und DSGVO-Elemente. Aus diesen kann inhaltlich wenig mitgenommen werden, weshalb es hier einer Verbesserung des Formats bedarf. Mit Blick auf das langfristige Ziel, dass die Annotationen gar nicht als Liste ausgegeben werden sollen, sondern direkt am entsprechenden Element des Softwaremodells annotiert werden, kann auf diesen Zwischenschritt gegebenenfalls verzichtet werden. Allerdings setzt die Annotation am Softwaremodell den eben beschriebenen Schritt der Transformation des Eingabemodells voraus. Darüber hinaus erfolgte die Ausgabe der Kommentare bisher

erst im Anschluss an die Erstellung des Instanzmodells. Übertragen auf die praktische Anwendung hieße dies, dass erst ein Softwaremodell entwickelt und dann im Nachhinein der Annotation unterzogen wird. Der Vorteil, durch die Annotationen bereits in einem frühestmöglichen Entwicklungsstadium datenschutzkonform zu modellieren, würde somit nicht zum Tragen kommen. Zielführender ist es, die Annotationen bereits während der Erstellung zu annotieren. Ob dies möglich ist oder die Annotation phasenweise erfolgen muss, ist Gegenstand zukünftiger Arbeit.

8.3. Überarbeitung des Kommentarmodells

Im Laufe der Erarbeitung entstand vermehrt die Problematik, die „Grundelement[e] der Rechtsnorm“ von den „Begriff[en]“ zu differenzieren (siehe zum Vergleich Abb. 5.1). Darüber hinaus scheint die Bezeichnung „Grundelement[e] der Rechtsnorm“ aus juristischer Sicht nicht ganz exakt. Beim Versuch, diesen beiden Problematiken zu begegnen, fiel auf, dass die Modellierung des Kommentarmodells möglicherweise vereinfacht werden könnte, da sich Beziehungen und Elemente doppeln. Eine mögliche Auflösung der Redundanzen besteht in der Abänderung des Kommentarmodells, wie sie in Abbildung 8.1 zu sehen ist. Durch diese Variante würde zugleich den beiden zuvor genannten Problematiken begegnet werden, ohne dass es zu inhaltlichen Veränderungen der Kommentarinstanzen kommt. Lediglich die Struktur und damit die Darstellungsweise würde sich verändern.

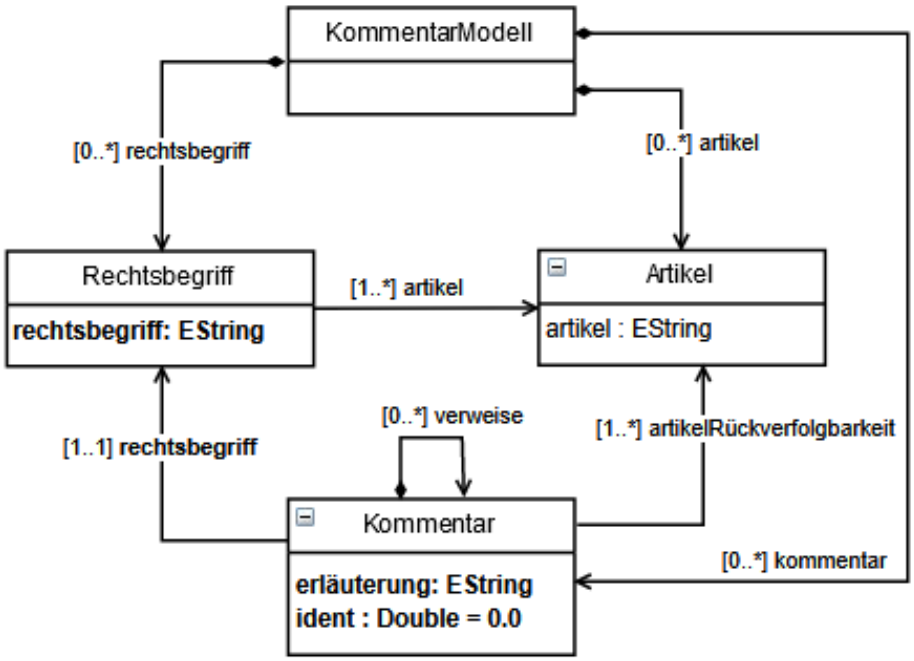


Abbildung 8.1.: Verändertes Kommentarmodell

Hinter der Modellierung mit Differenzierung der beiden Elemente lag zu Beginn der Arbeit der Gedanke, dass die „Grundelement[e] der Rechtsnorm“ eben jene Begriffe sind, die im Rechtsmodell (hier das DSGVO-Modell) modelliert sind - und die im Gegensatz zu den restlichen Begriffen für den späteren Vergleich im Annotationsmechanismus benötigt werden. Allerdings wurde der Annotationsmechanismus nun so implementiert, dass die Zuordnung der Kommentare zu den DSGVO-Instanzen über einen *instanceOf*-Vergleich erfolgt. Dadurch werden die gesuchten Elemente vom Programmierer festgelegt und müssen nicht zwangsläufig als gesonderte Elemente im Kommentarmodell erkennbar sein. Eine fehlende Differenzierung würde somit kein Problem für die Annotationen darstellen.

In zukünftiger Arbeit sollte diese Modelländerung noch einmal vollständig auf Funktionalität und Anwendbarkeit der Kommentare mit der veränderten Struktur geprüft werden. Sollte beides gleich oder gar positiver ausfallen als bisher, so spricht sowohl die Beseitigung der Redundanzen als auch die verbesserte Bezeichnung für diese Abänderung. In diesem Fall müssen alle Artefakte dieser Bachelorarbeit entsprechend der Modelländerung angepasst werden. Sowohl die Kommentar-Instanz als auch der Kommentarkatalog müssen umfassend überarbeitet werden.

8.4. Erweiterung der Kommentare

Bisher beinhalten die Kommentare nur reine Erläuterungen. Es stellt sich die Frage, ob der Kommentar in dieser Form bereits seine volle Wirksamkeit entfaltet oder ob eine Ergänzung um „Handlungsempfehlungen“ zielführender wäre. So würde dem Softwareentwickler nicht nur gesagt werden, worum es sich bei dem vorliegenden Objekt handelt, sondern auch direkt, wie er damit umgehen muss, um datenschutzkonform zu entwickeln. Gerade bei komplexen juristischen Sachverhalten könnte dies einen großen Vorteil mit sich bringen. Allerdings scheinen passende Handlungsempfehlungen auch nicht einfach zu geben zu sein. Sie hängen stark vom System, Kontext sowie der konkreten Stelle im System ab und können sich somit stark unterscheiden.

In zukünftiger Arbeit und insbesondere mit Blick auf die nächsten Entwicklungsschritten des Annotationsmechanismus kann überlegt werden, ob und wie solche Handlungsempfehlungen sinnvoll in die Kommentare integriert werden können.

9. Abschluss

In dieser Arbeit wurde ein Konzept zum automatisierten Annotieren rechtlicher Kommentare an einem DSGVO-Modell vorgestellt. Basierend auf einem Konzept zur systematischen Kommentierung bestehenden Rechts wurde ein Annotationsmechanismus eingeführt, der Elemente einer DSGVO-Modellinstanz mit datenschutzrechtlichen Kommentaren versieht. Abschließend wurde dieser Ansatz an einer Instanz einer Fallstudie evaluiert.

Die Arbeit gliederte sich in zwei Hauptteile. Im ersten Teil wurde ein umfassendes Konzept zur systematischen Kommentierung bestehenden Rechts entworfen. Unterschiedliche Ausgestaltungen wurden vorgestellt und gegeneinander abgewogen. Schließlich fiel die Entscheidung begründet auf den Verzicht der expliziten Darlegung der Auslegungsmethodik. Das Konzept diente als Basis des in Kapitel 5 konzipierten Kommentarmodells sowie des in Abschnitt 5.3 ausgearbeiteten Kommentarkatalogs. Festzuhalten bleibt, dass das Konzept allgemeine Gültigkeit besitzt, insbesondere da es sich in seinem Anwendungsgebiet nicht auf die Kommentierung eines spezifischen Gesetzestextes beschränkt.

Im zweiten Hauptteil stand schließlich die Entwicklung des Annotationsmechanismus im Zentrum. Eine Annotation besteht aus den zwei Teilen Kommentar und DSGVO-Element. Die Basis dieser beiden Teile wurde jeweils getrennt voneinander entwickelt, bevor sie anschließend im Annotationsmodell miteinander verknüpft wurden. Das Kommentarmodell spiegelte das Konzept zur systematischen Kommentierung in seinem Aufbau und den Einzelbestandteilen wieder. Eine aus diesem Modell erzeugte Instanz beinhaltete die einzelnen Kommentare der DSGVO. Aufgrund des Umfangs der DSGVO wurden sie zum einen auf die Bestandteile des DSGVO-Modells von Boltz et al. und zum anderen auf den Anwendungsbereich sowie die Zielgruppe der Softwareentwicklung beschränkt. Die formulierten Kommentare wurden zuzüglich der Kommentar-Instanz anschaulich in einem Kommentarkatalog zusammengetragen. Nachdem das Kommentarmodell vorgestellt wurde, wurde es schließlich mit dem DSGVO-Modell von Boltz et al. in einem neu konzipierten Annotationsmodell verknüpft. Jeweils ein Element aus jedem Modell bildeten eine Annotation. Durch dieses Modell war die Grundlage für eine automatisierte Annotation geschaffen.

Auf die Vorstellung der Basismodelle und -elemente, folgte die Einführung des Mechanismus' zum automatisierten Annotieren der Kommentare. Er basierte auf einem Vergleich des Typs des DSGVO-Elements mit der entsprechenden Bezeichnung des Bestandteils des rechtlichen Konzepts eines Kommentars und infolge dessen einer korrekten Zuordnung zu einem Element-Kommentar Paar. Ein solches wurde als Annotation bezeichnet. Gespeichert wurden alle Annotationen in einer Annotationsliste.

Evaluiert wurde die Konzeption des Ansatzes schließlich anhand einer DSGVO-Instanz der *Travel Planner Application*. Für diese Instanz wurde mittels des Annotationsmechanismus' eine vollständige und korrekte Annotationsliste generiert.

Trotz positiver Evaluation bezüglich der Testinstanz, wurden mehrere noch zu verbessernde Aspekte aufgedeckt. Sie machen weiterführende Arbeiten notwendig, um dem übergeordneten Anwendungsziel näher zu kommen. Beispielsweise konnte eine vereinfachte Zusammenarbeit des Rechts- und Softwarebereichs sowie die Nutzbarkeit in der Praxis des Softwareentwicklers mit dem hier entwickelten Ansatz und der Evaluation noch nicht gezeigt werden.

Zusammenfassend bleibt als Beurteilung des entwickelten Konzepts festzuhalten, dass die spezifischen Ziele dieser Arbeit - die Entwicklung eines Konzepts zum systematischen Kommentieren bestehenden Rechts sowie eines Konzeptes zum automatisierten Annotieren rechtlicher Kommentare an einem DSGVO-Modell - erreicht wurden. Die Annotation der Testinstanz erfolgte korrekt und funktionierte in dem gegebenen Rahmen. Allerdings bewegt sich der Ansatz noch nicht auf einem Level zur praktischen Anwendung in der Softwareentwicklung. Wie in Kapitel 8 ausgeführt, sind hierzu weiterführende Arbeiten einerseits notwendig, um die Transformation eines Softwaremodells in eine DSGVO-Instanz zu ermöglichen. Andererseits stehen noch umfassende Nutzerstudien für aussagekräftige Ergebnisse über die tatsächliche Unterstützung in der praktischen Anwendung, sprich der Entwicklung datenschutzkonformer Softwaremodelle, aus. Da der Ansatz seine Korrektheit und Nutzbarkeit unter den hier gegebenen Rahmenbedingungen gezeigt hat, dient er dennoch als solide Grundlage für weitere Entwicklungsschritte. Er bildet ein weiteres Artefakt in der Entwicklung eines ganzheitlichen Ansatzes zur eigenständigeren datenschutzkonformen Softwareentwicklung und vereinfachten Zusammenarbeit mit Rechtsexperten. Des Weiteren stellt das Konzept einen ergänzenden Beitrag in der Entwicklung, da ein verwandter Ansatz in der untersuchten Forschungsliteratur nicht gefunden werden konnte.

Abschließend sei noch einmal angemerkt, dass, auch bei hoher Funktionalität und erfolgreicher Nutzbarkeit in der Praxis, die Nutzung der automatisierten Annotation die Entwicklung datenschutzkonformer Softwaremodelle nicht von einer Rechtsprüfung durch einen Rechtsexperten befreit. Die Annotationen dienen nur als Unterstützung, nicht als Rechtsgrundlage.

Literatur

[1] Object Management Group (OMG). *Meta Object Facility (MOF) Specification*. Version 1.4.1. Formally published bey ISO as ISO/IEC 19502:2005(E). 2005. URL: https://www.omg.org/spec/MOF/ISO/19502/PDF.

[2] C. Atkinson und T. Kuhne. „Model-driven development: a metamodeling foundation". In: *IEEE Software* 20.5 (2003), S. 36–41. DOI: 10.1109/MS.2003.1231149.

[3] ISSE Uni Augsburg. *Travel Planner Application*. URL: https://kiv.isse.de/projects/iflow/TravelPlannerSite/index.html.

[4] Steffen Becker, Heiko Koziolek und Ralf Reussner. „The Palladio component model for model-driven performance prediction". In: *Journal of Systems and Software* 82.1 (2009). Special Issue: Software Performance - Modeling and Analysis, S. 3–22. ISSN: 0164-1212. DOI: https://doi.org/10.1016/j.jss.2008.03.066. URL: https://www.sciencedirect.com/science/article/pii/S0164121208001015.

[5] Barry W. Boehm, Robert K Mcclean und D. E. Urfrig. „Some experience with automated aids to the design of large-scale reliable software". In: *IEEE Transactions on Software Engineering* SE-1.1 (März 1975), S. 125–133. DOI: 10.1109/tse.1975.6312826. URL: https://doi.org/10.1109%2Ftse.1975.6312826.

[6] Nicolas Boltz u. a. „A Model-Based Framework for Simplified Collaboration of Legal and Software Experts in Data Protection Assessments". In: *P326 - INFORMATIK 2022 - Informatik in den Naturwissenschaften*. Hrsg. von Daniel Demmler, Daniel Krupka und Hannes Federrath. Gesellschaft für Informatik, Bonn, 2022, S. 521–532. DOI: 10.18420/inf2022_44.

[7] Eclipse Foundation. *Eclipse Modeling Framework*. URL: https://eclipse.dev/modeling/emf/.

[8] Robert France und Bernhard Rumpe. „Model-driven Development of Complex Software: A Research Roadmap". In: *Future of Software Engineering (FOSE '07)*. 2007, S. 37–54. DOI: 10.1109/FOSE.2007.14.

[9] Sascha Kremer u. a. „Datentransfer nach Art. 49 DSGVO: Was geht, wenn sonst nichts geht? — Gleichwertige Alternativen zu Angemessenheitsbeschluss und geeigneten Garantien nach unionsrechtlicher Auslegung". In: *Computer und Recht* 37.12 (2021), S. 784–796. DOI: doi:10.9785/cr-2021-371207. URL: https://doi.org/10.9785/cr-2021-371207.

[10] Mario Martini u. a. *Die DSGVO und das nationale Recht – Erste Überlegungen zum nationalen Regelungsbedarf*. Münster, Jan. 2016, S. 525. ISBN: 3956458907.

[11] Olaf Muthorst. „Auslegung: Eine Einführung". In: *Juristische Arbeitsblätter* 45.10 (2013), S. 721–727.

[12] Gabriel Pedroza u. a. „A Model-based Approach to Realize Privacy and Data Protection by Design“. In: *2021 IEEE European Symposium on Security and Privacy Workshops*. 2021, S. 332–339. DOI: 10.1109/EuroSPW54576.2021.00042.

[13] Stephan Seifermann u. a. „Detecting violations of access control and information flow policies in data flow diagrams“. In: *Journal of Systems and Software* 184 (2022), S. 111138. ISSN: 0164-1212. DOI: https://doi.org/10.1016/j.jss.2021.111138. URL: https://www.sciencedirect.com/science/article/pii/S0164121221002351.

[14] B. Selic. „The pragmatics of model-driven development“. In: *IEEE Software* 20.5 (2003), S. 19–25. DOI: 10.1109/MS.2003.1231146.

[15] Eduard Sing. „A Meta-Model Driven Method for Establishing Business Process Compliance to GDPR“. UNIVERSITY OF TARTU - Institute of Computer Science, Software Engineering Curriculum, Mai 2018.

[16] Laurens Sion u. a. „An Architectural View for Data Protection by Design“. In: *2019 IEEE International Conference on Software Architecture (ICSA)*. 2019, S. 11–20. DOI: 10.1109/ICSA.2019.00010.

[17] Herbert Stachowiak. „Der allgemeine Modellbegriff“. In: *Allgemeine Modelltheorie*. Springer Vienna, 1973, S. 128–303. DOI: 10.1007/978-3-7091-8327-4_3. URL: https://doi.org/10.1007%2F978-3-7091-8327-4_3.

[18] Jake Tom, Eduard Sing und Raimundas Matulevičius. „Conceptual Representation of the GDPR: Model and Application Directions: 17th International Conference, BIR 2018, Stockholm, Sweden, September 24-26, 2018, Proceedings“. In: Jan. 2018, S. 18–28. ISBN: 978-3-319-99950-0. DOI: 10.1007/978-3-319-99951-7_2.

[19] Damiano Torre u. a. „An AI-assisted Approach for Checking the Completeness of Privacy Policies Against GDPR“. In: *2020 IEEE 28th International Requirements Engineering Conference (RE)*. 2020, S. 136–146. DOI: 10.1109/RE48521.2020.00025.

[20] Damiano Torre u. a. „Model Driven Engineering for Data Protection and Privacy: Application and Experience with GDPR“. In: *CoRR* abs/2007.12046 (2020). arXiv: 2007.12046. URL: https://arxiv.org/abs/2007.12046.

[21] Damiano Torre u. a. „Using Models to Enable Compliance Checking Against the GDPR: An Experience Report“. In: *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*. 2019, S. 1–11. DOI: 10.1109/MODELS.2019.00-20.

[22] Amt für Veröffentlichungen der EU. *Charta der Grundrechte der Europäischen Union*. Website. EU. URL: http://data.europa.eu/eli/treaty/char_2012/oj.

[23] Amt für Veröffentlichungen der EU. *Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates*. Website. EU. URL: http://data.europa.eu/eli/reg/2016/679/oj.

[24] Amt für Veröffentlichungen der EU. *Zusammenfassung des Dokuments: Artikel 288 des Vertrags über die Arbeitsweise der Europäischen Union – Richtlinien*. Website. EU. URL: https://eur-lex.europa.eu/DE/legal-content/summary/european-union-directives.html.

[25] Heinrich Amadeus Wolff und Stefan Brink, Hrsg. *Beck'scher Online-Kommentar - Datenschutzrecht*. Website. München. URL: https://beck-online.beck.de/Bcid/Y-400-W-BECKOKDATENS.

[26] Heinrich Amadeus Wolff und Stefan Brink, Hrsg. *Datenschutzrecht: DS-GVO, BDSG, Grundlagen, bereichsspezifischer Datenschutz - Kommentar*. 2. Auflage. München: C.H. Beck, 2022.

A. Anhang

A.1. Kommentarkatalog

Tabelle A.1.: Kommentarkatalog

ID	Grundelement der Rechtsnorm	Artikel zur Rückverfolgbarkeit	Erläuterung	Verweise: Verknüpfte Begriffe	Verknüpfte Artikel	Verknüpfte Grundelemente der Rechtsnorm
1.0	Natürliche Person	Art. 4 Nr. 1 Komm.: Art. 4 Rn. 5	Die Natürliche Person ist eine lebende und von der juristischen Person abzugrenzende Person. Im Rahmen der DSGVO ist eine natürliche Person stets in ihrer identifizierbaren oder identifizierten Ausprägung zu verstehen. Sie wird auch als betroffene Person bezeichnet. Die personenbezogenen Daten, die sich auf die identifizierbare/ -zierte natürliche Person beziehen, fallen unter den Anwendungskontext der DSGVO und dürfen nur entsprechend der Bestimmungen verwendet werden.	Identifizerte/-bare Person Juristische Person Betroffene Person		
2.0	Dritter	Art. 4 Nr. 10 Komm.: Art. 4 Rn. 108-112	Beim „Dritten“ handelt es sich um eine natürliche oder juristische Person (privates o. öffentl. Recht), Behörde, Einrichtung oder andere Stelle. Durch die Begriffsbestimmung ist der „Dritte“ verschieden vom Verantwortlichen sowie der betroffenen Person und steht außerhalb der datenverarbeitenden Stelle. Bei der Weitergabe personenbezogener Daten an Dritte handelt es sich um eine Datenübermittlung. Somit fällt sie in den Anwendungsbereich der Verarbeitung.	Dritter Juristische Person Verantwortlicher		Natürliche Person

3.0	Verantwortlicher	Art. 4 Nr. 7 Komm.: Art. 4 Rn. 87-93	Beim Verantwortlichen handelt es sich um eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle. Verantwortliche besitzen allein oder gemeinsam mit anderen Entscheidungsbefugnis in Bezug auf die Zwecke und Mittel der Verarbeitung personenbezogener Daten. Sie sind Normadressat der DSGVO und unterliegen Pflichten (Art. 24 ff.). Letzteren zufolge, können mehrere Verantwortliche gemeinsam für die Verarbeitung zuständig sein. In diesem Fall können intern einzelne Zuständigkeitsbereiche aufgeteilt werden, während die Verantwortlichen extern weiterhin gemeinsam verantwortlich sind. Des Weiteren gilt, dass ein Auftragsdatenverarbeiter zwar auch den Rechten und Pflichten der DSGVO unterliegt, aber kein Verantwortlicher in dem hier genannten Sinne ist. Ein Verantwortlicher ist für die Einhaltung der Verarbeitungsgrundsätze verantwortlich und insbesondere rechenschaftspflichtig. Bei gemeinsamer Verantwortlichkeit muss gemeinsam festgelegt werden, wer welche Verpflichtung gemäß der DSGVO erfüllt (Rechte der betroffenen Person; Informationspflichten). Die vorausgesetzten Zwecke und Mittel können bei Bedarf durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben werden.	Informationspflicht Juristische Person Grundsätze der Verarbeitung	Art. 13 Art. 14 Art. 24 ff. (insb. Art. 26)	Natürliche Person

4.0	Daten	Art. 1 Abs. 1 Art. 4 Nr. 13, 14, 15 Komm.: Art. 4 Rn. 22-24 Komm.: Art. 4 Rn. 27b	Daten sind zentraler Gegenstand der DSGVO. Im Vordergrund steht der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie der freie Verkehr dieser Daten. Darüber hinaus gelten Sachdaten zunächst nicht als personenbezogene Daten, können aber in Abhängigkeit ihres Detaillierungsgrades und Kontextes einen Personenbezug erhalten. Synthetische Daten beziehen sich auf allgemein verwendbare Datensätze, die für die Erzeugung und Validierung von KI-Modellen genutzt werden können. Handelt es sich dabei um ausreichend anonymisierte Daten ohne Personenbezug, sind es keine personenbezogenen Daten.			
4.1	Personenbezogene Daten	Art. 4 Nr. 1 Komm.: Art. 4 Rn. 3-4 Komm.: Art. 4 Rn. 11-12	Personenbezogene Daten müssen von einer mindestens identifizierbaren natürlichen Person stammen und sich personenbezogen auf eben diese Person beziehen. Zu solchen Daten zählen Identifikationsmerkmale, äußere Merkmale, innere Zustände oder sachliche Informationen. Besonders sensible personenbezogene Daten wie genetische oder biometrische Daten und Gesundheitsdaten gelten als „besondere Kategorien personenbezogener Daten“ (Art. 9 DSGVO). Des Weiteren werden „personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten“ (Art. 10 DSGVO) ebf. abgegrenzt, da sie nur gesondert verwendet werden dürfen.	Personenbezogene Daten Natürliche Person Identifizierte/-bare Person Besondere Kategorien personenbezogener Daten und personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten	Art. 9 Art. 10	Daten

5.0	Verarbeitung	Art. 4 Nr. 2 Art. 5 Art. 6 Komm.: Art. 5 Rn. 2	Eine Verarbeitung im Rahmen der DSGVO umfasst unabhängig des verarbeitenden Subjekts oder der Verarbeitungsart (autom./ nicht-autom.) jeden ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten. Somit sind auch arithmetische oder logische Operationen in den Begriff der Verarbeitung eingeschlossen. Zur Verarbeitung im Sinne der DSGVO zählen: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung o.Ä., Abgleich, Verknüpfung, Einschränkung, Löschen, Vernichtung. Als rechtmäßig gilt eine Verarbeitung oder eine ihrer Unterformen, wenn der Aspekt der Rechtsgrundlage eingehalten ist. Darüber hinaus unterliegt die Verarbeitung personenbezogener Daten den verpflichtenden Grundsätzen der Datenverarbeitung.	Einschränkung der Verarbeitung Rechtmäßigkeitstatbestände Grundsätze der Verarbeitung	Rechtsgrundlage

5.1	Erhebung	Art. 4 Nr. 2 Art. 5 Abs. 1 lit. b Komm.: Art. 4 Rn. 35-41	Die Erhebung ist eine Form der Verarbeitung, wobei ihr Gegenstand immer personenbezogene Daten sind. Es handelt sich dabei um das Beschaffen von personenbezogenen Daten bei der betroffenen Person selbst. Der Vorgang muss mit ihrer Kenntnis sowie durch ihr persönliches Tun in schriftlicher, mündlicher, erklärender Form oder mittels nonverbalem Verhalten explizit erfolgen. Neben dem aktiven Part des Betroffenen bedarf die Erhebung eines aktiven, subjektiven Tuns der beschaffenden Stelle und darf somit nicht im Sinne von „zuwachsen“ an den Verantwortlichen herangetragen werden. Darüber hinaus muss die Erhebung für einen oder mehrere festgelegte, eindeutige und legitime Zwecke erforderlich sein. Die Methode der Datenerhebung selbst ist dabei irrelevant. Zudem muss die Informationspflicht gegenüber dem Betroffenen nach Art. 13 DSGVO beachtet werden. Wurden die Daten ohne Kenntnis der Betroffenen Person erhoben, so ist eine nachträgliche Benachrichtigung (Art. 19 DSGVO) notwendig. Kommt es hingegen zu einer unzulässigen Erhebung, dürfen die Daten nicht verwendet und gespeichert werden. Ist eine Speicherung bereits geschehen, sind die personenbezogenen Daten aus diesem Grund unverzüglich zu löschen. Darüber hinaus gilt: Als Unteraspekt der Verarbeitung müssen ebenfalls die Bedingungen ebendieser erfüllt sein.	Betroffene Person Informationspflicht Personenbezogene Daten Verantwortlicher	Art. 13 Art. 19	Verarbeitung

5.2	Speicherung	Art. 4 Nr. 2 Art. 5 Abs. 1 lit. c Art. 5 Abs. 1 lit. e Komm.: Art. 4 Rn. 42-42a	Eine Speicherung erfolgt durch das Erfassen und Aufnehmen personenbezogener Daten auf einem Datenträger mit dem Ziel der weiteren Verarbeitung oder Nutzung. Hierzu zählt auch das analoge Aufbewahren dieser Daten durch Lagerung in Akten. Die Stelle, bei der die Daten gelagert werden, gilt ebenfalls als eine Instanz, die Daten im Sinne der DSGVO verarbeitet und unterliegt den entsprechenden Pflichten und Rechten. Da es auf den tatsächlichen Umgang mit den Daten nicht ankommt, stellen auch bloß gespeicherte bzw. gelagerte Daten eine Verarbeitung im Sinne der DSGVO dar. Des Weiteren sind im Rahmen der „Grundsätze für die Verarbeitung personenbezogener Daten“ die Speicherbegrenzung sowie die Datenminimierung einzuhalten. Darüber hinaus gilt: Als Unteraspekt der Verarbeitung müssen ebenfalls die Bedingungen ebendieser erfüllt sein.	Erfassen und Aufnehmen Einschränkung der Verarbeitung Speicherbegrenzung Datenminimierung	Verarbeitung

5.3	Transfer	Art. 4 Nr. 2 Komm.: Art. 4 Rn. 49-51 Komm.: Art. 4 Rn. 52	Ein Transfer von Daten besteht in der Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener Daten an Dritte. Dabei ist die Form der Weitergabe und die Anzahl der empfangenden Dritten nicht entscheidend. Unter dem Transferbegriff ist die Übermittlung von der bloßen Weitergabe von Daten an einen Empfänger zu unterscheiden und die Aktivität geht - entgegen der „Bereitstellung“ - vom Sender aus. Eine Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen ist nur auf der Basis eines Angemessenheitsbeschlusses (Art. 45 Abs. 3 DSGVO) möglich. Liegt kein Beschluss vor, so ist eine Übermittlung unter geeigneten Garantien (Art. 46 DSGVO) möglich. Liegt keines von beidem vor, so sind Ausnahmefälle zu prüfen. Des Weiteren spielt es keine Rolle, ob die Übermittlung innerhalb der Union und damit der DSGVO geschieht oder eine Verknüpfung zu einem außerhalb davon liegenden Drittstaat aufweist. Darüber hinaus gilt: Als Unteraspekt der Verarbeitung müssen ebenfalls die Bedingungen ebendieser erfüllt sein.	Empfänger Verknüpfung Weitergabe Ausnahmefälle der Übermittlung an Drittländer	Art. 44-46 Art. 49	Verarbeitung
5.4	Verwendung	Art. 4 Nr. 2 Komm.: Art. 4 Rn. 48 Erwägungsgrund 50	Hierbei handelt es sich um einen Auffangtatbestand, der jede Form der Verarbeitung umfasst. Insbesondere jene, die in der DSGVO nicht explizit erwähnt werden. Darüber hinaus gilt: Als Unteraspekt der Verarbeitung müssen ebenfalls die Bedingungen ebendieser erfüllt sein.			Verarbeitung

6.0	Zweck	Art. 5 Abs. 1 lit. b Art. 5 Abs. 1 lit. c Art. 5 Abs. 1 lit. e Art. 6 Abs. 1 UAbs. 1 Art. 6 Abs. 4 Komm.: Art. 6 Abs. 1 Rn. 24	Die Datenverarbeitung personenbezogener Daten ist eng mit Zwecken verknüpft. Damit sie legitimiert ist, muss sie den Zweckbindungsgrundsatz erfüllen. Dafür notwendige Verarbeitungszwecke werden vom Verantwortlichen oder der Union bzw. deren Mitgliedstaaten festgelegt. Eine Weiterverarbeitung in unvereinbarender Weise mit den festgelegten Zwecken ist nicht erlaubt. Ausnahmen werden in Art. 89 Abs. 1 DSGVO formuliert. Darüber hinaus definiert der Grundsatz weitere Maßgaben wie Speicherdauer u.Ä. und bildet die Basis für die Entscheidung über Angemessenheit und Erheblichkeit der Verarbeitung. Dies bedeutet, dass die erhobenen personenbezogenen Daten dem Zweck angemessen, für den Verarbeitungszweck erheblich und ihm entsprechend auf das notwendige Maß beschränkt sein müssen. Doch nicht nur Verarbeitungszwecke müssen festgelegt werden, sondern jeder dieser Zwecke muss von der Rechtsgrundlage gedeckt sein und dementsprechend auf einem Rechtmäßigkeitstatbestand beruhen. Eine Einwilligung als Form der Rechtsgrundlage kann nur zu vorher definierten Zwecken gegeben werden und gilt ausschließlich für diese eingewilligten Zwecke. Um der Informationspflicht nachkommen zu können, müssen die Zwecke bereits vor der Verarbeitung festgelegt sein. Für den Präzisionsgrad der Zweckfestlegung gibt es keine Vorgaben, doch der Betroffene muss nachvollziehen können, für welche Zwecke seine Daten erhoben werden. Kommt es zu einer Zweckänderung, so muss die Vereinbarkeit mit dem Erhebungszweck geprüft werden. Vom Grundsatz der Zweckbindung ist eine Zweckänderung nur ausgenommen, wenn dieser in einer Einwilligung zugestimmt wurde, sie durch eine Rechtsvorschrift erlaubt ist oder öffentl. interessante Archivzwecke, wissenschaftl. oder hist. Forschungszwecke oder stat. Zwecke relevant werden. Liegt eine solche Ausnahme nicht vor, kann der Verantwortliche die Daten nur erneut unter geänderte Zweckfestlegung erheben.	Zweck Zweckbindung Datenminimierung Richtigkeit Informationspflicht Rechtmäßigkeitstatbestände Erhebungszweck	Art. 89 Abs. 1	Rechtsgrundlage

7.0	Rechtsgrundlage	Art. 5 Art. 6 Art. 6 Abs. 3 Komm.: Art. 5 Rn. 6 Komm.: Art. 6 Abs 1 Rn. 10 Komm.: Art. 6 Abs. 1 Rn. 24	Grundsatz der DSGVO ist das generelle Verbot einer Verarbeitung personenbezogener Daten, sofern sie nicht durch einen Erlaubnistatbestand einer Rechtsvorschrift legitimiert ist (Verbot mit Erlaubnisvorbehalt). In der Rechtsgrundlage wird die Tragweite und Anwendung der Datenverarbeitung personenbezogener Daten dargelegt. Sie muss so präzise geregelt sein, dass sie für den Betroffenen voraussehbar ist und der Zweck der Verarbeitung muss eindeutig daraus hervorgehen sowie festgelegt sein. Je nach zugrundeliegendem Rechtmäßigkeitstatbestand ist sie durch Unionsrecht oder das Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, festgelegt. Für eine rechtmäßige Verarbeitung personenbezogener Daten müssen zum einen die „Grundsätze der Verarbeitung personenbezogener Daten“ eingehalten werden. Für diese Einhaltung besteht eine Rechenschafts- sowie Nachweispflicht durch den Verantwortlichen. Zum anderen muss einer der sechs Rechtmäßigkeitstatbestände pro Verarbeitungszweck erfüllt sein. Zu beachten ist, dass eine Einwilligung als Rechtmäßigkeitstatbestand nicht eingeholt werden darf, wenn auch ein anderer Rechtmäßigkeitstatbestand greifen würde. Darüber hinaus gelten Rechtmäßigkeitsanforderungen wie bspw. Betroffenenrechte (Art. 12-23 DSGVO) oder Datensicherheitsmaßnahmen (Art. 32-39 DSGVO). Ausnahmen dieser Rechtsgrundlage sind nur im Rahmen besonderer Verarbeitungssituationen (Art. 85 ff. DSVGO) durch Rechtsvorschriften der Mitgliedstaaten möglich.	Rechtmäßigkeitstatbestände Prüfung Zweckvereinbarkeit Grundsätze der Verarbeitung Nachweis-/ Rechenschaftspflicht	Art. 12-23 Art. 32-39 Art. 85-91

7.1	Vertragserfüllung	Art. 6 Abs. 1 lit. b Art. 7 Abs. 4 Art. 49 Abs. 1 lit. b Komm.: Art. 6 Abs. 1 UAbs. 1 lit. b Rn. 40-47	Die Verarbeitung personenbezogener Daten kann zur Erfüllung eines Vertrags mit dem Betroffenen als Vertragspartei oder für die Durchführung vorvertraglicher Maßnahmen erforderlich sein. Dieser Rechtmäßigkeitstatbestand bezieht sich sowohl auf Verträge als auch vertragsähnliche Konstellationen, die auf willentliche Erklärungen des Betroffenen zurückzuführen sind (z.B. Gefälligkeitsverhältnisse). Ein Vertrag unterliegt einem allgemeinen Kopplungsverbot. Das bedeutet, der Vertrag darf den Freiwilligkeitsaspekt der Einwilligung nicht beeinträchtigen und die personenbezogene Datenverarbeitung muss erforderlich sein. Der Vertragspartner und der datenverarbeitende Verantwortliche müssen dabei nicht personenidentisch sein. Ist eine Verarbeitung personenbezogener Daten durch unbeteiligte Dritte erforderlich, kann auch dies im Rahmen des Vertragstatbestandes legitimiert sein. Kommt es zu einer Änderung des Vertrags, resultiert dies in einem „neuen“ Vertrag. Auch für einen Vertrag oder vorvertragliche Maßnahmen unterliegt die Verarbeitung personenbezogener Daten dem Maßstab der Erforderlichkeit. Die Erforderlichkeit bezieht sich ebenso auf die möglichen Alternativen zum Vertrag, die dem Verantwortlichen zur Verfügung stehen. Geprüft wird, ob sie zumutbar sind und bspw. die Einwilligung eine adäquatere Verarbeitungsgrundlage darstellt, da diese dem Widerrufsrecht unterliegt und somit im Sinne des Betroffenen ist. Zwischen der Verarbeitung und dem konkreten Vertragszweck muss ein unmittelbarer Zusammenhang bestehen. Die erhobenen Daten unterliegen dem Verarbeitungsgrundsatz der Datenminimierung und Speicherbegrenzung. Eine Verarbeitung personenbezogener Daten im Rahmen vorvertraglicher Maßnahmen ist auch dann legitimiert, wenn es nicht zum Vertragsabschluss kommt.	Kopplungsverbot Datenminimierung Einwilligung Informationspflicht Nachweis/ Rechenschaftspflicht Grundsätze der Verarbeitung Rechtmäßigkeitstatbestände Speicherbegrenzung Zweckbindung Vertrag Vorvertragliche Maßnahmen	Rechtsgrundlage

7.2	Ausübung der öffentlichen Gewalt/ Behörde	Art. 6 Abs. 1 lit. e Art. 6 Abs. 3 Komm.: Art. 6 Abs. 1 UAbs. 1 Rn. 53-62 Komm.: Art. 6 Abs. 1 UAbs. 1 Rn. 65	Ist eine Verarbeitung zur Erfüllung einer Aufgabe erforderlich, die dem Verantwortlichen übertragen wurde und im öffentliche Interesse liegt oder durch eine öffentliche Gewalt erfolgt, so ist sie rechtmäßig. Eine öffentliche Gewalt kann ein Verantwortlicher, Auftragsverarbeiter, Empfänger, Dritter oder die (betroffene) Aufsichtsbehörde sein. Der handelnde Akteur hingegen bleibt unbestimmt. Zum Tatbestand der Verarbeitung personenbezogener Daten im öffentlichen Interesse gehören unter anderem Aufgaben, die einem von der Union anerkannten Ziel im allgemeinen Interesse entsprechen. So beispielsweise auch wenn eine solche Verarbeitung die Straßenverkehrssicherheit verbessert. Als Normadressaten gelten bei dieser Rechtsgrundlage nur jene Verantwortlichen, denen eine solche Aufgabe nach Art. 6 Abs. 1 lit. e DSGVO übertragen wurde und nicht dritte Empfänger der Daten. Öffentliche Behörden sind von gewissen Bestimmungen ausgenommen bzw. besitzen Ausnahmerechte. So dürfen sie nicht auf den Tatbestand der „Verarbeitung zur Wahrung berechtiger Interessen“ (Art. 6 Abs. 1 lit. f DSGVO) zurückgreifen. Andererseits gilt das Recht auf Löschung bei ihren Verarbeitungstätigkeiten nicht, wenn die Verarbeitung zur Wahrnehmung einer Aufgabe in Ausübung einer öffentlichen Gewalt erfolgt. Die Bestimmung der Erforderlichkeit gestaltet sich hier als anspruchsvoll, da bestimmt werden muss, welche Daten die adressierte Stelle als Informationsgrundlage benötigt, um die Aufgabe zu erfüllen. Die Rechtsgrundlage für eine Verarbeitung zur Wahrnehmung einer Aufgabe, die in Ausübung öffentlicher Gewalt erfolgt, wird durch Unionsrecht oder mitgliedstaatliches Recht (des Verantwortlichen) festgelegt. Für sie gelten im Rahmen der Datenschutz-Folgenabschätzung (Art. 35 Abs. 10) gesonderte Regelungen.	Datenschutz-Folgenabschätzung	Art. 6 Abs. 1 lit. f Art. 6 Abs. 1 lit. e Art. 35 Abs. 10

7.3	Einwilligung	Art. 4 Nr. 11 Art. 6 Abs. 1 lit. a Art. 7 Art. 8	Der Verantwortliche muss die Einwilligung, die im Falle der Schriftform in verständlicher, leicht zugänglicher Form ausgestellt sowie in klarer, einfacher Sprache formuliert ist, nachweisen können. Liegt eine Einwilligung vor, ist die Verarbeitung für die darin definierten Zwecke und ausschließlich für diese rechtmäßig. Kommt es zu einer Zweckänderung der in der Einwilligung festgehaltenen Zwecke, muss aus diesem Grund die Vereinbarkeit ebendieser geprüft und gegebenenfalls eine erneute Einwilligung eingeholt werden. Wurde die Einwilligung im Zusammenhang eines Vertrages gegeben, so muss eine Freiwilligkeitsbeurteilung hinsichtlich der Notwendigkeit der Verarbeitung der geforderten personenbezogenen Daten erfolgen (Kopplungsverbot). Der Betroffene hat ein jederzeitiges Widerrufsrecht, über welches der Verantwortliche ihn im Sinne der Informationspflicht im Zuge der Einwilligung informieren muss. Wurde die Einwilligung widerrufen, bleibt die bisherige Verarbeitung rechtmäßig, aber alle auf Grundlage der Einwilligung verarbeiteten Daten sind zu löschen. Ausnahme: Die Verarbeitung wurde von vornherein auf eine andere Rechtsgrundlage gestützt. Handelt es sich bei der einwilligenden Person um eine Minderjährige, so ist die Verarbeitung der personenbezogenen Daten des Kindes nur rechtmäßig, sofern dieses das sechszehnte Lebensjahr vollendet hat oder die Einwilligung durch Personen mit elterlichem Sorgerecht gegeben wurde. Die verantwortliche Stelle ist in der Pflicht, angemessene Anstrengungen zur Kontrolle zu unternehmen.	Einwilligung Kopplungsverbot Informationspflicht Nachweis/ Rechenschaftspflicht Zweck	Rechtsgrundlage Vertragserfüllung

8.0	Nachweis	Art. 5 Abs. 2 Art. 6 Abs. 1 lit. a Art. 7 Abs. 1 Art. 24 Abs. 1 Komm.: Art. 5 Rn. 37-39 Komm.: Art. 7 Rn. 89-91	Der Verantwortliche unterliegt einer Nachweis- und Rechenschaftspflicht. So ist er für die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten verantwortlich und muss diese nachweisen können. Beruht die Verarbeitung auf einer Einwilligung, muss er auch diese nachweisen können. Andernfalls gilt die Einwilligung als nicht wirksam erteilt. Für die Sicherstellung und den Nachweis, dass die Verarbeitung DSGVO konform erfolgt, müssen geeignete technische und organisatorische Maßnahmen ergriffen werden. Dabei ist die Art des Nachweises nicht festgelegt, Textformen und elektronische Dokumentationen bieten allerdings die größte Rechtssicherheit. Die Nachweispflicht kann nur durch eine Dokumentation oder ein Daten-Managementsystem erfüllt werden, welche für mind. drei Jahre aufbewahrt werden muss.	Einwilligung Grundsätze der Verarbeitung

A.2. Glossar

Tabelle A.2.: Glossar zu („Verknüpfte Begriffe“)

Begriff	**Artikel zur Rückverfolgbarkeit**	**Erläuterung**
Aufsichtsbehörde	Art. 4 Nr. 21 Art. 4 Nr. 22 Art. 55 Art. 57 Art. 58	Eine vom Mitgliedstaat eingerichtete staatliche Stelle, die die einheitliche Anwendung der DSGVO überwacht. Zur Erfüllung ihrer Aufgaben (Art. 57 DSGVO) hat sie eine Reihe an Befugnissen (Art. 58 DSGVO). Dazu gehört auch die betroffene Aufsichtsbehörde. Sie ist von der Verarbeitung personenbezogene Daten betroffen, wenn der Verantwortliche oder Auftragsverarbeiter im Mitgliedstaat der Aufsichtsbehörde ansässig ist, die Verarbeitung Auswirkungen auf Betroffene mit Wohnsitz im Mitgliedstaat der Aufsichtsbehörde hat oder eine Beschwerde an diese Aufsichtsbehörde gerichtet wurde.
Ausnahmefälle der Übermittlung an Drittländer	Art. 49 Abs. 1	Die Übermittlung ist bei Fehlen eines Angemessenheitsbescshlusses oder geeigneter Garantien unter folgenen Aspekten möglich: a) Ausdrückliche Einwilligung des Betroffenen nach einer Risikoaufklärung b) Vertragserfüllung zwischen Betroffenem und Verantwortlichem/ vorvertragliche Maßnahmen auf Antrag des Betroffenen c) Abschluss/ Erfüllung eines Vertrags zwischen Verantwortlichem und natürlicher/ jurist. Person d) öffentliches Interesse e) Rechtsansprüche f) Schutz lebenswichtiger Interessen, sofern der Betroffene nicht im Stande ist, eine Einwilligung zu geben g) Übermittlung aus einem Register, welches unter bestimmten Bedingungen zur Einsicht offensteht.

Besondere Kategorien personenbezogener Daten und personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten	Art. 9 Art. 10 Komm.: Art. 4 Rn. 182-183	Besondere Kategorien personenbezogener Daten benennen insbesondere genetische, biometrische und Gesundheitsdaten sowie jene Daten, aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen und Daten zum Sexualleben oder der sexuellen Orientierung, sofern sie Aufschluss über die Identität einer Person geben. Ihre Verarbeitung ist untersagt, es sei denn es treffen die in Art. 9 Abs. 2 DSGVO genannten Fälle zu. Bspw. wenn eine Einwilligung vorliegt oder die Verarbeitung aus Rechten und Pflichten des Arbeits-/ Sozialschutzrechts erwächst. Eine Verarbeitung von Daten über strafrechtliche Verurteilungen sowie Straftaten darf nur unter behördlicher Aufsicht oder wenn das Unionsrecht bzw. mitgliedstaatliches Recht dies zulässt, geschehen.
Betroffene Person	Art. 15-18 Komm.: Art. 4 Rn. 28	Bei der betroffenen Person handelt es sich um die identifizierte/ identifizierbare natürliche Person, die davor zu schützen ist, dass ihr Persönlichkeitsrecht durch den Umgang mit ihren personenbezogenen Daten beeinträchtigt wird. Sie ist weder Verantwortlicher, noch Dritter und kann Rechte in Bezug auf ihre personenbezogenen Daten geltend machen (Art. 15-18 DSGVO).
Betroffenenrechte	Art. 6 Abs. 1 lit. e/ f Art. 12-23	Die betroffene Person hat das Recht auf eine transparente Information und Kommunikation ihrer Rechte. Diese bestehen unter anderem in der Informationspflicht durch den Verantwortlichen und das Recht auf Auskunft. Darüber hinaus kann sie ihren Anspruch auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit geltend machen. Zudem besitzt sie das Recht auf jederzeitigen Widerspruch der Verabeitung nach Art. 6 Abs. 1 lit. e oder f DSGVO.

Datenminimierung	Art. 5 Abs. 1 lit. c Komm.: Art. 5 Rn. 24-26	Dieser Grundsatz besagt, dass personenbezogene Daten auf ein für den (bei der Erhebung festehenden) Zweck der Verarbeitung erforderliches Mindestmaß reduziert sowie dafür angemessen sein müssen. Eine Verarbeitung zu rein hypothetischen Zwecken ist unangemessen.
Datenschutz-Folgenabschätzung	Art. 35 Komm.: Art. 35 Abs. 3 Rn. 25-29	Wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss der Verantwortliche im Voraus der Verarbeitung eine Abschätzung der Folgen vornehmen. Sofern vorhanden, sollte der Rat des Datenschutzbeauftragten eingeholt werden. Eine solche Folgenabschätzung ist insbesondere für folgende drei Fallgruppen erforderlich: wenn a) in automatisierter Weise eine systematische Bewertung persönlicher Aspekte natürlicher Personen vorgenommen wird, b) eine Verarbeitung besonderer Kategorien personenbezogene Daten oder von Daten strafrechtlicher Verurteilungen und Straftaten getätigt wird, c) es sich um eine systematische Überwachung öffentlich zugänglicher Bereiche handelt.
Dritter	Art. 4 Nr. 10 Komm.: Art. 4 Rn. 108-112	Beim „Dritten“ handelt es sich um eine natürliche oder juristische Person (privates o. öffentl. Recht), Behörde, Einrichtung oder andere Stelle. Ausgenommen ist die betroffene Person, der Verantwortliche, der Auftragsverarbeiter und jene Personen, denen eine unmittelbare Verantwortung zur Verarbeitung der personenbezogenen Daten übertragen wurde.
Einschränkung der Verarbeitung	Art. 4 Nr. 3 Art. 18 Abs. 2 Art. 89 Komm.: Art. 4 Rn. 58	Gespeicherte personenbezogene Daten werden markiert, um ihre zukünftige Verarbeitung einzuschränken. Nur unter besonderen Bedingungen darf auf die Daten zugegriffen werden (siehe Art. 18 Abs. 2 DSGVO). In automatisierten Dateisystemen ist zu beachten, dass technische Mittel zur Einschränkung so eingesetzt werden müssen, dass die personenbezogenen Daten nicht weiterverarbeitet oder verändert werden können. Die Archivierung ist von der Einschränkung zu unterscheiden und wird gesondert behandelt (Art. 89 DSGVO).

Einwilligung	Art. 4 Nr. 11	Als Einwilligung gilt jede zeitlich vorhergehende, freiwillige, informierte, formgemäße und unmissverständlich abgegebene Willensbekundung einer einwilligungsfähigen Person. Diese kann in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung durch die betroffene Person geschehen, mit welcher sie ihr Einverständnis zur Verarbeitung ihrer personenbezogene Daten gibt. Die Einwilligung beschränkt sich auf die darin definierten Inhalte und Zwecke.
Empfänger	Komm.: Art. 4 Rn. 49	Werden Daten innerhalb der verantwortlichen Stelle, zwischen dieser und einer im Auftrag tätigen Stelle oder vom Betroffenen empfangen, so handelt es sich jeweils um einen Empfänger und keinen Dritten.
Erhebungszweck	Komm.: Art. 6 Abs. 4 Rn. 96-101	Vor oder bei der Erhebung festgelegter Verwendungszweck.
Grundsätze der Verarbeitung	Art. 5 Komm.: Art. 5 Rn. 2	Die Grundsätze der Datenverarbeitung sind verpflichtend und unterteilen sich wie folgt: Abs. 1: a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; b) Zweckbindung; c) Datenminimierung; d) Richtigkeit; e) Speicherbegrenzung; f) Integrität und Vertraulichkeit; Abs. 2: Rechenschaftspflicht

Identifizierte/ -bare Person	Art. 4 Nr. 1 Komm.: Art. 4 Rn. 14-21	Eine natürliche Person, die insbesondere mittels Zuordnung zu einer Kennung direkt oder indirekt identifiziert werden kann. Zur Feststellung müssen alle Mittel berücksichtigt werden, die nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden. Es ist hierbei nicht entscheidend, dass die Daten zur Identifizierung in einer Hand liegen.
Informationspflicht	Art. 13 Art. 14	Der Verantwortliche hat die Pflicht, zum einen den Betroffenen zum Zeitpunkt der Erhebung personenbezogene Daten gemäß den Anforderungen zu informieren. Kommt es zu einer Weiterverarbeitung zu einem anderen Zweck, so hat der Verantwortliche den Betroffenen wiederum gemäß den Richtlinien zu informieren. Werden die Daten nicht direkt beim Betroffenen erhoben, so teilt der Verantwortliche, sofern es sich nicht als unmöglich erweist, die Daten gemäß Art. 14 DSGVO mit.
Juristische Person	Komm.: Art. 4 Rn. 5	Juristische Personen sind keine einzelnen natürlichen Personen, sondern ein Zusammenschluss von mehreren natürlichen oder juristischen Personen. Juristische Personen des Privatrechts (bspw. Stiftungen, GmbH) werden nicht ausdrücklich als Betroffene von der DSGVO erfasst. Sie müssen sich als Verarbeiter etc. jedoch gleichermaßen an die DSGVO halten.
Kopplungsverbot	Komm.: Art. 7 Abs. 4 Rn. 42-50	Die Erfüllung eines Vertrags wird von der Einwilligung in eine Datenverarbeitung abhängig gemacht, die für die Vertragserfülllung nicht notwendig ist.
Nachweis/ Rechenschaftspflicht	Art. 5 Abs. 2 Art. 6 Abs. 1 lit. a Komm.: Art. 7 Rn. 89-91	Der Verantwortliche ist für die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten verantwortlich und muss diese nachweisen können. Beruht die Verarbeitung auf einer Einwilligung, muss er auch diese nachweisen können. Andernfalls gilt die Einwilligung als nicht wirksam erteilt.

Natürliche Person	Komm.: Art. 4 Rn. 5	Die DSGVO stellt nur auf natürliche Personen im Sinne von identifizierten oder identifizierbaren natürlichen Personen ab. Sie werden auch als „betroffene Person“ bezeichnet.
Öffentliche Behörde Öffentliche Gewalt	Art. 4 Art. 6 (Abs. 1 lit. e)	Kann ein Verantwortlicher, Auftragsverarbeiter, Empfänger, Dritter oder eine (betroffene) Aufsichtsbehörde sein.
Personenbezogene Daten	Art. 4 Nr. 1	Sind eben solche Informationen, die sich auf eine identifizierte/ -bare natürliche Personen beziehen.
Prüfung Zweckvereinbarkeit	Art. 6 Abs. 4	Liegt der Verarbeitung ein anderer als der Erhebungszweck zugrunde und besteht keine Einwilligung oder Rechtsvorschrift, so muss der Verantwortliche eine Zweckvereinbarkeitsprüfung durchführen. Hierbei wird die Verbindung zwischen dem Erhebungszweck und dem neuen Zweck, der Zusammenhang der Erhebung der personenbezogene Daten, die Art der personenbezogene Daten, mögliche Folgen der Weiterverarbeitung und das Vorhandensein geeigneter Garantien berücksichtigt.
Rechtmäßigkeitstatbestände	Art. 6 Abs. 1 UAbs. 1	a) Einwilligung zur Verarbeitung b) notwendig für Vertragserfüllung/ vorvertragliche Maßnahmen c) Erfüllung einer rechtlichen Verpflichtung d) lebenswichtige Interessen e) öffentliches Interesse f) berechtigtes Interesse
Rechtsgrundlage	Komm.: Art. 6 Abs 1 Rn. 10	Die Rechtsgrundlage besteht aus sechs Rechtmäßigkeitstatbeständen, von denen mindestens einer erfüllt sein muss, um eine rechtmäßige Verarbeitung darzustellen. Zugrundeliegende Rechtsgrundlagen werden ggf. durch Unionsrecht oder vom Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, festgelegt. In der Rechtsgundlage muss der Zweck der Verarbeitung festgelegt werden.

Richtigkeit	Art. 5 Abs. 1 lit. d	Personenbezogene Daten müssen sowohl sachlich richtig als auch auf dem neuesten Stand sein. Ist dies nicht der Fall, so müssen angemessene Maßnahmen getroffen werden, um die personenbezogene Daten, die in Hinblick auf ihre Zwecke inkorrekt sind, zu berichtigen oder zu löschen.
Speicherbegrenzung	Art. 5 Abs. 1 lit. e Art. 89 Abs. 1 Komm.: Art. 5 Rn. 32-34	Dieser Grundsatz fordert eine Beschränkung der Speicherdauer auf ein unbedingt erforderliches Mindestmaß, welches sich nach der Zweckerreichung richtet. Demnach darf die Form der Datenspeicherung eine Identifikation des Betroffenen nur so lange ermöglichen, wie es der Verarbeitungszweck erfordert. Anschließend folgt eine Löschung aus Eigeninitiative des Verarbeiters. Eine Vorratsspeicherung für noch unbestimmte Zwecke ist nicht erlaubt. Aus der Nachweispflicht folgt eine zumindest interne Festlegung der Speicherdauer. Eine erlaubte Ausnahme zur längeren Speicherung personenbezogene Daten besteht, sofern diese unter Berücksichtigung geeigneter Maßnahmen (Art. 89 Abs. 1 DSGVO) ausschließlich für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden.
Verantwortlicher	Art. 4 Nr. 7 Art. 24 ff.	Beim Verantwortlichen handelt es sich um eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle. Er entscheidet allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten. Letztere können durch das Unionsrecht oder durch das Recht der Mitgliedstaaten vorgegeben sein. Verantwortliche sind Normadressat der DSGVO (Pflichten definiert ab Art. 24 ff.).

Verarbeitung	Art. 4 Nr. 2	Verarbeitung bezeichnet jeden ausgeführten Vorgang im Zusammenhang mit personenbezogene Daten unabhängig der Zuhilfenahme automatisierter Verfahren. Hierzu zählen: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung o.Ä., Abgleich, Verknüpfung, Einschränkung, Löschen, Vernichtung.
Verknüpfung	Komm.: Art. 5 Rn. 52	Daten aus einem System werden mit einem anderen verbunden oder ihm hinzugefügt, um den anderen Datensätz zu vervollständigen.
Vertrag	Komm.: Art. 6 Abs. 1 UAbs. 1 lit. b Rn. 40-47	Ein Vertrag erfasst rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnisse, bei denen der Betroffene eine Vertragspartei darstellt und muss eine Zweckfestlegung beinhalten. Der Nachweis der Wirksamkeit eines Vertrages liegt in der Pflicht des Verantwortlichen. Gestaltet er sich aufgrund verschiedenartiger Pflichten und Rechte komplex, so muss er für eine datenschutzrechtliche Beurteilung ggf. aufgeschlüsselt werden.
Vertragserfüllung	Art. 6 Abs. 1 lit. b	Die Verarbeitung personenbezogene Daten ist zur Erfüllung eines Vertrags mit dem Betroffenen als Vertragspartei oder für die Durchführung vorvertraglicher Maßnahmen erforderlich. Darin eingeschlossen sind Leistungs-, Neben- und Rücksichtspflichten.
Vorvertragliche Maßnahmen	Komm.: Art. 6 Abs. 1 UAbs. 1 lit. b Rn. 40-47	Im Zentrum steht hier die Vorbereitung und Anbahnung eines Vertrages (z.B. Vertragsverhandlungen). Eine Verabeitung personenbezogene Daten auf dieser Grundlage kann nur legitimiert sein, wenn sie auf Anfrage des Betroffenen erfolgt.
Weitergabe	Komm.: Art. 4 Rn. 49	Die Weitergabe von personenbezogene Daten besteht zwischen dem Verantwortlichen und einem Empfänger. Sie unterliegt dem Erfordernis der Zweckbindung und Erforderlichkeit.

Zweck	Art. 5 Abs. 1 lit. b Art. 6 Abs. 1 UAbs. 1	Der Zweck übernimmt u.A. mit dem Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DSGVO) eine zentrale Rolle in der DSGVO und bildet die Grundlage einer rechtmäßigen Verarbeitung personenbezogene Daten. Ein Zweck gilt als rechtmäßig, wenn seine Rechtsgrundlage auf mindestens einem der Rechtmäßigkeitstatbestände (Art. 6 Abs. 1 UAbs. 1 DSGVO) beruht. Zwecke der Verarbeitung werden vom Verantwortlichen oder der Union bzw. deren Mitgliedstaaten festgelegt.
Zweckbindung	Art. 5 Abs. 1 lit. b Art. 89 Abs. 1	Personenbezogene Daten müssen für mindestens einen festgelegten, eindeutigen und legitimen Zweck erhoben werden. Eine Weiterverarbeitung in nicht vereinbarender Weise mit diesem Zweck ist nicht erlaubt. Eine Ausnahme hiervon bildet die Weiterverarbeitung iSv. Art. 89 Abs. 1 DSGVO.