i2v

bmvit

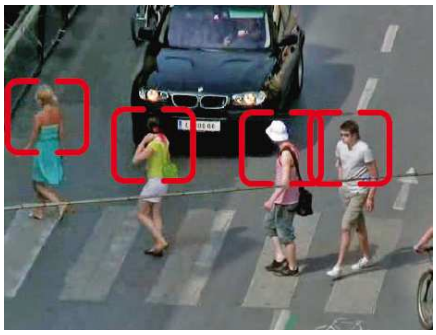
Bundesministerium
für Verkehr,
Innovation und Technologie

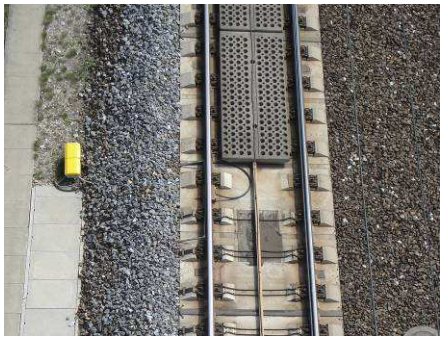
Juergen

Juristische Rahmenbedingungen für die Erfassung, Verarbeitung, Verbreitung und Benutzung von intermodalen Verkehrsinformation durch Dritte für Mobilitätsinformationsdienstleistungen

Eine Studie finanziert im Rahmen der 2. Ausschreibung der Programmlinie i2v des Forschungs- und Technologieprogramms iv2splus

Juli 2010





iv2splus

FFG

Impressum:

Herausgeber und Programmverantwortung:

Bundesministerium für Verkehr, Innovation und Technologie

Abteilung Mobilitäts- und Verkehrstechnologien

Renngasse 5

A - 1010 Wien

Für den Inhalt verantwortlich:

ABC Consulting

Gartengasse 19a/4

1050 Wien

Programmmanagement IV2Splus

Österreichische Forschungsförderungsgesellschaft mbH

Bereich Thematische Programme

Sensengasse 1

A – 1090 Wien

Juergen

Juristische Rahmenbedingungen für die Erfassung, Verarbeitung, Verbreitung und Benutzung von intermodalen Verkehrsinformation durch Dritte für Mobilitätsinformationsdienstleistungen

Eine Studie finanziert im Rahmen der 2. Ausschreibung der Programmlinie i2v des Forschungs- und Technologieprogramms iv2splus

AutorInnen:

DI Alexander Chloupek

DI (FH) Kathrin Morawetz MSc.

Mario Lange BSc.

DI Jürgen Zajicek

DI Melitta Dragaschnig

DI Katja Schechtner

Martin Höfner MSc.

MMag. Ewald Lichtenberger

Dr. Jens Eckhardt

Auftraggeber: Bundesministerium für Verkehr, Innovation und Technologie

Auftragnehmer: DI Alexander Chloupek

Inhaltsverzeichnis

Einleitung....8
1. Bestehende verkehrstelematische Schwerpunkte....9
2. Projektschwerpunkte Juergen....11
3. Rechtliche Grundlagen....13
3.1 Datenschutz....14
3.1.1 Anwendungsbereich....14
3.1.2 Grundsätze des Datenschutzrechts....14
3.1.3 Datenschutzrechtliches Verständnis von Erheben und Verwenden personenbezogener Daten....16
3.1.4 Meldepflicht, Vorabkontrolle und Beauftragter für den Datenschutz sowie Datengeheimnis....17
3.1.5 Technische und organisatorische Maßnahmen („IT-Sicherheit“)....19
3.1.6 Rechte der Betroffenen....19
3.1.7 Auftragsdatenverarbeitung....20
3.1.8 Zulässigkeit der Datenverwendung nach deutschem Recht....21
3.1.9 Exkurs: Arbeitnehmerrechte....22
3.1.10 EU-Hintergrund....23
3.1.11 Exkurs: Geodatenrichtlinie....24
3.1.12 Exkurs: Neuerungen im österreichischen DSG....25
3.1.13 Exkurs: Videoüberwachung....25
3.2 Immaterialgüterrechte....28
3.2.1 Patentrecht....28
3.2.2 Urheberrecht....30
3.3 Vertragsrechtliche Aspekte....32
3.3.1 Leistungsbeschreibung (Quality of Service und Verfügbarkeit)....33
3.3.2 Sekundärrechte....34
3.3.3 Lieferantenbeziehung....34
3.3.4 Vertrieb....35
4. Telematikanwendungen in den einzelnen Verkehrsmodi....36
4.1 Straßenverkehr....36

4.1.1 Verkehrszustandserfassung 37
4.1.2 Enforcement 44
4.2 Schienenverkehr 49
4.2.1 Infrastrukturmessstellen 50
4.2.2 Location Based Services 52
4.3 (Binnen)Schifffahrt 54
4.4 Luftfahrt 56
4.5 Intermodaler Verkehr 57
5. Der Umgang mit personenbezogenen Daten – Aktuelle Themenbereiche 59
5.1 Verkehrsdatenerfassung mit Mobiltelefonen 59
5.1.1 MASI Active 59
5.2 Mautsysteme 60
5.2.1 Schaffung der Grundlage für ein einheitliches Mautsystem 60
5.2.2 Die Weiterverwertung von Mautdaten 60
5.2.3 Fazit 62
5.3 Das Filmen von Personen 62
5.3.1 Google Street View in Österreich 62
5.3.2 Google Street View in Deutschland 63
5.3.3 Stations- und U-Bahnüberwachung der Wr. Linien 64
6. Handlungsempfehlungen 65
7. Conclusio 66
Literaturverzeichnis 67
Rechtsgrundlagen 68
Internetquellen 69
Abbildungsverzeichnis 70
Tabellenverzeichnis 70
Abkürzungsverzeichnis 71

Die Bezeichnungen sollen immer geschlechtsneutral verstanden werden.

Kurzfassung

Bei der Erfassung, Verarbeitung, Verbreitung und Benutzung von intermodalen Verkehrsinformationen durch Dritte kommt eine Vielzahl von Rechtsmaterien zum Tragen, die sich in unterschiedlichen Rechtsquellen finden. Ein eigenes „Verkehrstelematik- und Verkehrsinformations-Gesetzes“ besteht nicht. Vor Allem das Datenschutzrecht, das Vertragsrecht und das Immaterialgüterrecht (Patentrecht, Urheberrecht) bilden die wesentlich betroffenen Rechtssphären. Die Untersuchung der betroffenen Rechtsgebiete für definierte Anwendungsfälle in den Themenbereichen der einzelnen Verkehrsmodi erfolgte entlang eines typischen Projektablaufs. Aus den Erfahrungen der beteiligten Partner wurden bestehende Applikationen und Systeme analysiert. Ausgehend von diesen exemplarischen Anwendungen wurden durch die beteiligten Partner gemeinsam einerseits zwingend anzuwendende Rechtsbestimmungen und andererseits durch rechtliche Bestimmungen (Verträge) abzusichernde wirtschaftliche Interessen herausgearbeitet.

Datenbeschaffung (rechtliches Schwerpunktthema: Datenschutz) – Datensicherung und -aufbereitung (rechtliches Schwerpunktthema: Immaterialgüterrecht) – als auch Datenverwertung (rechtliches Schwerpunktthema: Vertragsrecht) waren im Zentrum der Rechtsanalysen. Weiters wurden auch der Schutz von Gewerblichen Schutzrechten im weiteren Sinn („Know-How“), die Richtlinie 2007/2/EG zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft, nationale Interessen der Öffentliche Sicherheit („Heimatschutz“) – der oft im Wiederspruch zum Datenschutz steht (Stichwort Vorratsdatenspeicherung) – Informationsweiterverwendungsgesetz, Konsumentenschutz, Fahrgastrechte und öffentlich-rechtliche Bestimmungen, die den Ordnungsrahmen des Verkehrs bilden – bspw. Eisenbahnbuchgesetz, Straßenverkehrsordnung (StVO, KFG, etc.) analysiert.

Im Themenbereich „Straßenverkehr“ wurden die juristischen Rahmenbedingungen für Verkehrszustandserfassungen (z.B. FLEET und GO-SMART) und Videoerfassung von Daten (LPR und Personenerfassung) analysiert und auf Basis der Rechtsgrundlagen erläutert. Im Bereich „Schienenverkehr“ wurden die Rechtssphären von Infrastrukturmessstellen, wie zum Beispiel RFID und Lokalisierungsservices (GPS) untersucht. DoRIS als wichtigste Applikation in der Binnenschifffahrt wurde im Rahmen einer gesonderten Studie betrachtet und ist nicht Inhalt dieser Studie. Zur Luftfahrt wurden allgemeine Rechtsgrundlagen untersucht, da hier zum größten Teil firmeninterne Tools zur Anwendung kommen. Ein Schwerpunkt im Projekt „Juergen“ wurde auf intermodale Services (am Beispiel von ITS Vienna Region) gelegt, da hier besonders viele Überschneidungen der einzelnen Rechtssphären auftreten und damit die Auflösung der juristischen Gegebenheiten sowie kritische Rechtspunkte sich sehr gut darlegen lassen.

Auf Basis der durchgeführten Recherchen und Analysen der relevanten Applikationen sowie Rechtsbereiche ergaben sich im Abschlussteil der Studie Handlungsempfehlungen für die Verkehrstelematik in Hinsicht auf deren Rechtsaspekte.

Abstract

For the collection, handling, dispersion and use of intermodal traffic information by third parties a number of legal issues are concerned. A specific “Traffic telematics and traffic information law” does not exist. Particularly the data privacy law, contract law and the intangible property rights (patent, copyright) represent the substantially affected legal spheres. The analysis of the affected legal domains for the defined applications in the different modes of transport took place along a typical project process. From the experiences of the participating partners existing applications and systems were analyzed. Based on these exemplary applications mandatory provisions of the law as well as general contract law (necessary to take care of economic interests) have been evaluated.

The most important topics within the legal analysis were data collection (legal focus: Data Protection) – data storage and preparation (legal focus: Intangible Property Law) - and data dispersion (legal focus: contract law). Furthermore, also the protection of intellectual property rights in the broad sense ("Know-How"), Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community, national interests of the Public Security ("Homeland") – which often is contrary to privacy (keyword data retention) – information transfer law, consumer protection, passenger rights and public law provisions which constitute the regulatory framework of transport - for example, railway act, Road Traffic Regulations (Highway Code, CFG, etc.) were analyzed.

Within the road traffic domain the legal framework for traffic condition observations (e.g. FLEET and GO-SMART) and video recording of data (LPR and persons recording) were evaluated and discussed on legal grounds. For rail traffic infrastructure, monitoring applications such as RFID and localization based Services (GPS) were analyzed. DoRIS as the most important application in inland water traffic is analyzed within a separate study and is not within the scope of this study. For aviation, general legal grounds have been investigated, as here primarily in-house tools are being used. One focus of the project Juergen was laid on intermodal services (on the example of ITS Vienna Region), because of the overlapping of the different legal problems where critical legal issues can be evaluated very well.

Based on the research and analysis of the relevant applications and areas of law, recommendations for the traffic telematics field in terms of its legal aspects, were given, which are to be found in the conclusion part of this report.

Einleitung

Verkehrsinformationen können auf unterschiedlichen Wegen generiert und aus unterschiedlichen Quellen gewonnen werden. Das PIARC ITS Handbook beschreibt dazu die wichtigsten ITS Entwicklungen für den Straßenverkehr weltweit und verweist auf die internationale Entwicklung von ITS Systemen. Die ITS Architektur stellt hierzu den einheitlichen Standard für Intelligente Verkehrssysteme dar und sichert die Schnittstellen zu anderen Entwicklungen, Systemen und Moden.

Aus den Erfahrungen der beteiligten Partner werden im ersten Teil dieser Arbeit bestehende Applikationen und Systeme analysiert. Ausgehend von diesen exemplarischen Anwendungen werden durch die beteiligten Partner gemeinsam einerseits zwingend anzuwendende Rechtsbestimmungen und andererseits durch rechtliche Bestimmungen (Verträge) abzusichernde wirtschaftliche Interessen herausgearbeitet. Diese Rechtsbestimmungen werden im darauf folgenden Teil auf die exemplarisch ausgewählten Sachverhalte angewendet. Aus der Anwendung der Rechtsbestimmungen können als Ergebnis eventuelle Defizite des bestehenden Rechtsrahmens abgeleitet und legistische Vorschläge zur Verbesserung erarbeitet werden.

Dieses Dokument kann als Basis für die Einarbeitung in Rahmenpläne (z.B. Telematikrahmenplan) und Gesetze dienen oder einen eigenen Rechtsrahmen für die Erfassung, Verarbeitung, Verbreitung und Benutzung von intermodalen Verkehrsinformationen durch Dritte für Mobilitätsinformationsdienstleistungen darstellen. Speziell im Forschungs- und Entwicklungsbereich bestehen oft Unsicherheiten oder Fehlvorstellungen hinsichtlich der relevanten Rechtsvorschriften. So scheint unter anderem nicht immer bekannt zu sein, dass sowohl bei Teststellungen innerhalb von Forschungs- und Entwicklungsprojekten, als auch bei Regelfällen dieselben datenschutzrechtlichen Vorschriften gelten und etwa für Teststellungen keine Ausnahmen bestehen. Oftmals sehen sich F&E Projektdurchführende durch die geltenden Rechtsvorschriften in ihrem Projekt eingeschränkt oder behindert.

Die vorliegende Arbeit besteht aus sechs Kapiteln, die sich wie folgt zusammensetzen: Kapitel 1 beschreibt bereits bestehende verkehrstelematische Schwerpunkte aus unterschiedlichen Literaturquellen. Kapitel 2 erläutert, basierend auf Kapitel 1, die für das Projektteam aktuell und in naher Zukunft wichtig erscheinenden Themengebiete, welche in weiterer Folge innerhalb des Dokuments detaillierter behandelt werden. In Kapitel 3 werden, vorbereitend auf die Analysen der Rechtsbereiche einzelner gewählter Entwicklungen im darauf folgenden Kapitel, die rechtlich relevanten Grundlagen für die Erfassung, Verbreitung und Benutzung von Verkehrsinformationen dargestellt. Das vierte Kapitel erläutert anhand von Beispielen für Mobilitätsdienstleistungen die jeweils betroffenen Rechtsgebiete und zeigt Lösungen für eventuelle Problembereiche auf. In Kapitel 5 werden aktuelle, medienpräsente Themenbereiche behandelt, welche die Erfassung, Weitergabe und Verarbeitung personenbezogener Daten thematisieren. Zum Abschluss werden in Kapitel 6 Handlungsempfehlungen erläutert und die Conclusio präsentiert.

1. Bestehende verkehrstelematische Schwerpunkte

Bei der ganzheitlichen Betrachtung des Begriffes der Verkehrstelematik müssen auch die Schnittstellen zwischen den einzelnen Verkehrsmodi betrachtet werden. Als grundlegende Quellen konnten bei den Recherchearbeiten folgende Definitionen, welche die wichtigsten Bereiche der Verkehrstelematik aufgliedern, ausfindig gemacht werden.

Im **ITS Action Plan** der Europäischen Kommission von Dezember 2008 werden 6 sogenannte Priority Areas definiert:

- Optimale Nutzung von Straßen-, Verkehrs- und Reisedaten
- Kontinuität von Verkehrs- und Frachtenmanagement-ITS-Systemen auf Europäischen Transportkorridoren und in Ballungsräumen
- Straßensicherheit (und -sicherung)
- Integration des Vehikels in die Transportinfrastruktur
- Datenhaftung und Datenschutz
- Europäische ITS-Kooperation und Koordination

Diese Priority Areas bilden die Grundlage für die Maßnahmen, die innerhalb des Action Plans umgesetzt werden sollen, um den Einsatz von intelligenten Transportsystemen im Straßenverkehr inklusive der Schnittstellen mit anderen Verkehrsmodi zu koordinieren und beschleunigen.

Im **Freight Transport Logistic Action Plan** der Europäischen Kommission aus dem Jahr 2007 werden folgende Themenbereiche definiert:

- e-Freight und Intelligent Transport Systems (ITS)
- Nachhaltige Qualität und Effizienz
- Vereinfachung der Verkehrsketten
- Fahrzeugabmessungen und Belade-Standards
- Grüne Korridore für den Güterverkehr
- Städtische Güterverkehrslogistik

In dem Buch **„Mobilität Telematik Recht“** werden nachstehende Bereiche als die wesentlichen Schwerpunkte der Verkehrstelematik angeführt:

- Sicherheit im Verkehr
- Effiziente Nutzung des Verkehrsraums
- ÖPNV–Attraktivierung durch Telematik
- Aktuelle Verkehrsinformationen (TMC, etc.)
- Ökologische & ökonomische Einsparungspotentiale

Weitere Begriffsdefinitionen werden im Rahmen von **Vorlesungen** mit verkehrstelematischen Schwerpunkten an unterschiedlichen europäischen Universitäten und Hochschulen publiziert.

Im Rahmen der Vorlesung „Verkehrstelematik“, die am Informatik Institut der Universität Leipzig angeboten wird, werden folgende zentrale Themen der Verkehrstelematik behandelt:

- Telematik für die Verkehrsinfrastruktur
    - Grundlagen der Verkehrstheorie
    - Verkehrsdatenerfassung
    - Verkehrsinformation
    - Verkehrsprognosen
    - Verkehrsleitsysteme
    - Zahlungssysteme
- Telematik für den allgemeinen Individualverkehr
    - Routenplanungssysteme
    - Karteneinpassung (Map Matching)
    - Car-to-Car Kommunikation
- Telematik für den kommerziellen Individualverkehr
    - Tracking & Tracing
    - Tourenplanung
    - Container Terminal Logistik
- Telematik für den Öffentlichen Verkehr
    - Reiseinformationssysteme
    - Rechnergestützte Betriebsleitsysteme
    - Bezahlsysteme
    - Bedarfsabhängiger Betrieb
    - Car Sharing

Ähnliche dem Projektteam bekannte Unterlagen zu „Verkehrstelematik“-Vorlesungen gibt es an der Universität für Bodenkultur in Wien, der FH Technikum Wien und der Fachhochschule des bfi Wien.

Die oben angeführten Einteilungen sind stark subjektiv, weshalb sich das Projektteam in den folgenden Kapiteln, auf die derzeit am wichtigsten erscheinenden Themenbereiche festgelegt hat.

2. Projektschwerpunkte Juergen

Abbildung 2-1 zeigt eine Übersicht über die inhaltlichen Schwerpunkte im Projekt Juergen.

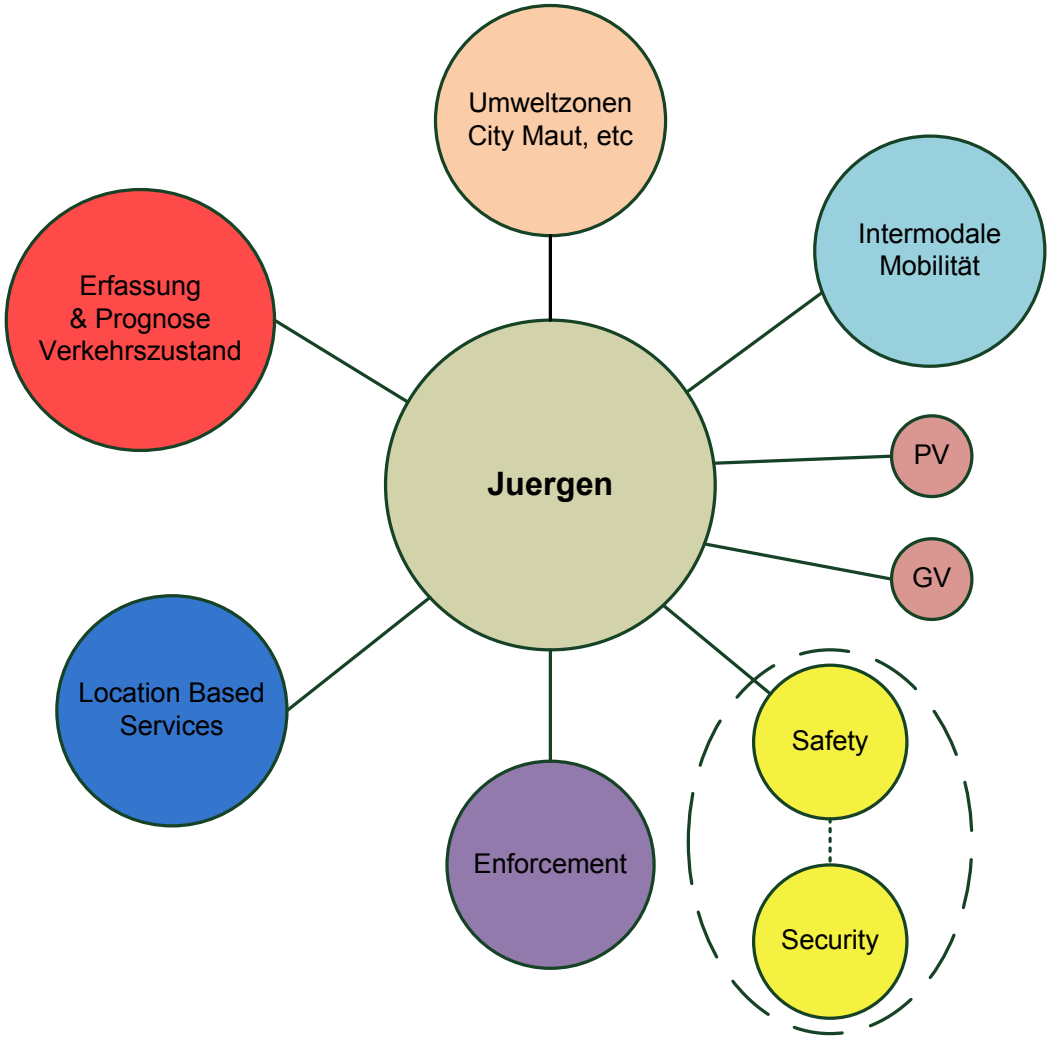


Abbildung 2-1: Projektschwerpunkte

Ausgehend von dieser Grafik werden in den weiteren Kapiteln Definitionen der Subkategorien vorgestellt sowie Anwendungsbeispiele zu den folgenden Projektschwerpunkten angeführt und rechtlich analysiert:

- Verkehrszustandserfassung/Erfassung/Prognose
    - FLEET und
    - GO-SMART
    - Infrastrukturmessstellen
    - DoRIS
- Enforcement und Safety
    - Rotlichtüberwachung und

    - Schutzwegüberwachung
- Location Based Services
    - GPS
- Intermodale Mobilität
    - AnachB.at

3. Rechtliche Grundlagen

Aus rechtlicher Sicht sind Telematik-Projekte mehrschichtig zu betrachten, wobei Überschneidungen möglich sind.

- Aus rechtlicher Sicht muss zunächst die Beschaffung der erforderlichen Daten rechtskonform sein. Diese betrifft insbesondere datenschutzrechtliche Fragen, aber auch möglicherweise Rechte Dritter an den verwendeten Daten (z. B. Datenbanken, also das Urheberrecht).
- Hieran schließt sich die rechtliche Bewertung der Aufbereitung der Informationen an. Dabei geht es um die Sicherung der Rechte zur Verwertung der Entwicklung, wobei das zu sichernde „Asset“ in den zusammengestellten und/oder aufbereiteten Informationen als solche und/oder in der „Technologie“ zu ihrer Generierung bestehen kann. Dieser Aspekt schließt neben den beispielsweise datenschutzrechtlichen Fragestellungen auch Fragen des Patent- und /oder Urheberrechts ein.
- Die wirtschaftliche Verwertung der Informationen und/oder der Technologie setzt voraus, dass der „Entwickler“ rechtliche Nachahmungen – jedenfalls für einen gewissen Zeitraum – unterbinden kann. Dies kann auf tatsächlicher Ebene durch Geheimhaltung oder auf rechtlicher Ebene durch Schutzrechte und Verträge erfolgen. Patente und Urheberrechte sind mögliche Grundlagen für den rechtlichen Schutz des „Assets“.
- Im Rahmen der wirtschaftlichen Verwertung kommen dann auch vertragliche Regelungen zu den Abnehmern hinzu, die über die vorgenannte Sicherung der wirtschaftlichen Verwertung hinausgehen. Hier geht es insbesondere um gesetzliche Regelungen zum Schutz des Abnehmers wie (Mängel-)Haftung, Informationspflichten, u. ä.
- Es müssen mit den „Abnehmern“ Verträge geschlossen werden, die einen sinnvollen Ausgleich zwischen den Risiken der Beteiligten darstellen. Der „Anbieter“ wird beispielsweise seine Haftung begrenzen wollen, weil ihm die Ungenauigkeit seiner Datengrundlage bekannt ist.

Überschneidungen ergeben sich dabei in vielfacher Hinsicht, weil jede der benannten Rechtsmaterien zwar einen zeitlich unterschiedlichen Relevanzschwerpunkt hat, aber sich im Regelfall über die gesamte Projektphase erstreckt. Aus datenschutzrechtlicher Sicht kann beispielsweise die geplante Verwertung Auswirkungen auf die Zulässigkeit der Beschaffung der Daten haben. Dasselbe gilt auch für die Entstehung von Schutzrechten zur Sicherung des Absatzes, da es einen erheblichen Unterschied machen kann, ob die verwendeten Daten selbst generiert werden oder auf durch Dritte generierte Daten zurückgegriffen wird. Ebenso hat die Qualität der Beschaffung und auch der Aufbereitung der Daten Auswirkungen auf die Sinnhaftigkeit von Haftungsbegrenzungen beim Absatz.

Um die Relevanz der Rechtsmaterien für ein Projekt bestimmen zu können, müssen diese jeweils für sich geprüft werden. Dementsprechend werden diese als Grundlage nachfolgend jeweils einzeln dargestellt.

3.1 Datenschutz

Nachfolgende Unterkapitel erläutern die relevanten Kapitel des Datenschutzes in Österreich mit Vergleichen zu Deutschland.

3.1.1 Anwendungsbereich

Die Grundlage für die Anwendung des Datenschutzrechts ist nach die Betroffenheit personenbezogener Daten.

Laut § 4 Z 1 DSG 2000 sind „personenbezogene Daten“ Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. „Nur indirekt personenbezogen“ (dies ist eine österreichische Besonderheit) sind Daten, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann. Personenbezogene Daten sind nach deutschem Recht (vgl. § 3 Abs. 1 BDSG) „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Damit ist zugleich der Begriff des Betroffenen für das deutsche Datenschutzrecht legal definiert. Sogenannte nur indirekt personenbezogene Daten kennt das BDSG nicht. Als Grenze der Anwendung wird daher die Anonymität bzw. das Anonymisieren zu verstehen sein. Anonymisieren ist nach § 3 Abs. 6 BDSG „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“.

3.1.2 Grundsätze des Datenschutzrechts

Das Datenschutzrecht ist insbesondere von drei Grundsätzen geprägt:

- Verbot mit Erlaubnisvorbehalt
- Grundsatz der Zweckbindung
- Transparenzgebot

Gemäß § 6 Abs. 1 DSG 2000 dürfen Daten in **Österreich** nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;

4. so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

Der Grundsatz des Verbots mit Erlaubnisvorbehalt ergibt sich im deutschen Datenschutzrecht aus § 4 BDSG:

> „*Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat".*

Vereinfacht gesagt bedeutet das: Jede Erhebung und / oder Verwendung personenbezogener Daten ist unzulässig, es sei denn, es liegt die Einwilligung des Betroffenen vor oder eine gesetzliche Regelung gestattet dies.

Das Gebot der Transparenz ist grundlegend in § 4 Abs. 3 BDSG verankert:

> *Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über*
>
> 1. *die Identität der verantwortlichen Stelle,*
> 2. *die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und*
> 3. *die Kategorien von den Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,*
>
> *zu unterrichten."*

Als Bestandteil der Transparenz ist der Grundsatz der Direkterhebung nach § 4 Abs. 2 BDSG („personenbezogene Daten sind beim Betroffenen zu erheben") zu verstehen, wobei § 4 Abs. 2 BDSG auch Ausnahmen hiervon vorsieht. Als Bestandteil der Transparenz im weiteren Sinne ist die Pflicht zu verstehen, dass bei einer Erhebung von Daten aufgrund einer gesetzlichen Grundlage die verantwortliche Stelle den Zweck, für den die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen hat (§ 28 Abs. 1 S 2 BDSG).

Der Grundsatz der Zweckbindung des deutschen Datenschutzrechts lässt sich aus den beiden vorgenannten Aspekten ableiten. Der Grundsatz der Zweckbindung sieht vor, das personenbezogene Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit dieser Zweckbestimmung nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Damit ist zunächst die Speicherung auf Vorrat – d. h. für noch nicht bekannte Zwecke – verboten. Des Weiteren führt der Grundsatz dazu, dass Daten zu einem anderen als dem ursprünglichen Zweck nicht verwendet werden dürfen, es sei denn, es liegt die Einwilligung des Betroffenen vor oder es ergreift ein gesetzlicher Zulässigkeitstatbestand ein.

3.1.3 Datenschutzrechtliches Verständnis von Erheben und Verwenden personenbezogener Daten

Laut § 7 Abs. 1 DSG dürfen Daten nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

Laut § 7 Abs. 2 DSG dürfen Daten nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und

2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und

3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 6 eingehalten werden.

Die Arten des Umgangs mit personenbezogenen Daten sind in § 3 Abs. 3 bis 6a BDSG umfassend definiert:

> *„(3) Erheben ist das Beschaffen von Daten über den Betroffenen.*
>
> *(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:*
>
> *1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,*
>
> *2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,*
>
> *3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass*
>
> *a) die Daten an den Dritten weitergegeben werden oder*
>
> *b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,*
>
> *4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,*
>
> *5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.*

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“

Die Definitionen im deutschen Datenschutzrecht zeigen, dass es keinen Umgang mit personenbezogenen Daten gibt, der kraft Definition außerhalb des Anwendungsbereichs des Datenschutzrechts stattfinden könnte (vgl. § 3 Abs. 5 BDSG).

Die Unterscheidung der Begrifflichkeiten ist deshalb von Bedeutung, weil das Datenschutzrecht in gesetzlichen Zulässigkeitsregelungen teilweise nur bestimmte Formen des Umgangs mit personenbezogenen Daten zulässt oder einen solchen fordert.

Im österreichischen Datenschutzrecht ist der Begriff des Verarbeitens weiter als in Deutschlang (vgl. § 4 Z 9 DSG 2000): Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten. Diese Unterschiedlichkeit in der Begrifflichkeit ist bei datenschutzrechtlich relevanten Anwendungen in beiden Ländern entsprechend zu beachten.

3.1.4 Meldepflicht, Vorabkontrolle und Beauftragter für den Datenschutz sowie Datengeheimnis

Vor der Aufnahme jeder Datenanwendung ist eine Meldung an die Datenschutzkommission zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten (zum Verfahren siehe §§ 16-22 DSG 2000). Die Meldepflicht trifft den Auftraggeber. Meldungen an das Datenverarbeitungsregister werden mittels Formblättern auf http://www.dsk.gv.at/site/6296/default.aspx getätigt. Die Meldung ist auch auf elektronischem Wege möglich.

Dabei gibt es folgende Ausnahmen von der Meldepflicht:

- Anwendungen, die ausschließlich veröffentlichte Daten enthalten,
- nur indirekt personenbezogene Daten erfassen
- oder für sogenannte Standard- oder Musteranwendungen wie in der STMV2000 definiert.

Die Meldepflicht nach deutschem Recht bestimmt sich nach § 4 BDSG. Der rechtliche Grundsatz ist die Pflicht zur Meldung von Verfahren automatisierter

Verarbeitungen. Der praktische Regelfall ist, dass eine Ausnahme von dieser Meldepflicht greift.

§ 4d Abs. 1 bis 4 BDSG enthält ein Regel-Ausnahme-Rückausnahmesystem. Vereinfacht lässt sich das wie folgt zusammenfassen: Grundsätzlich sind Verfahren automatisierter Verarbeitung vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde mit den nach § 4e BDSG festgelegten Inhalten zu melden (§ 4d Abs. 1 BDSG). Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat (§ 4d Abs. 2 BDSG). Des Weiteren entfällt die Meldepflicht, „wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei [ab dem 01.04.2010: in der Regel] höchstens neun Personen [ab dem 01.04.2010: ständig] mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt oder entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist“.

§ 4d Abs. 4 BDSG enthält wiederum Rückausnahmen von den vorgenannten Befreiungen. Die Befreiung besteht nicht, „wenn es sich um automatisierte Verarbeitung handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle 1. zum Zweck der Übermittlung, 2. zum Zweck der anonymisierten Übermittlung oder 3. für Zwecke der Markt- oder Meinungsforschung gespeichert werden“. Eine sogenannte Vorabkontrolle ist in § 4d Abs. 5 BDSG festgelegt: „Soweit automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten für der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle)“. § 4d Abs. 95 BDSG sieht vor, dass – eine weitere unter dort genannten Voraussetzungen – eine Vorabkontrolle insbesondere durchzuführen ist, wenn besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) verarbeitet werden oder die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistungen oder seines Verhaltens. Zuständig für die Vorabkontrolle ist grundsätzlich der Beauftragte für den Datenschutz (§ 4d Abs. 6 BDSG).

§ 4f, 4g BDSG regeln die Bestellung und die Aufgaben des sogenannten Beauftragten für den Datenschutz. Die Pflicht zur Bestellung eines Beauftragten für den Datenschutz ist in § 4f BDSG in Form eines Regel-Ausnahme-Verhältnisses festgelegt. Da die Bestellung eines Datenschutzbeauftragten kein Bestandteil der Frage der Zulässigkeit einer Erhebung oder Verwendung personenbezogener Daten ist, wird auf die Pflicht zur Bestellung und die Rolle des Beauftragten für den Datenschutz nicht näher eingegangen.

Das Datengeheimnis ist in § 5 BDSG verankert: „Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer

Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort“.

3.1.5 Technische und organisatorische Maßnahmen („IT-Sicherheit“)

Für alle Organisationseinheiten gilt in Österreich, dass Auftraggeber und Dienstleister Datensicherheit gewährleisten müssen. Sie müssen sicherstellen, dass Daten vor zufälliger oder unrechtmäßiger Zerstörung oder Verlust geschützt sind, ihre Verwendung ordnungsgemäß erfolgt und die Daten Unbefugten nicht zugänglich sind.[1]

Die Grundlage für Datensicherheit ist in Deutschland ist § 9 BDSG (samt Anlage):

> *„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“*

Nach der Anlage zu § 9 BDSG sind Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie Trennung verschiedener Daten nach unterschiedlichen Zwecken (Trennungsgebote) zu ergreifen. Die Begriffe sind in der Anlage jeweils definiert.

Für den Telekommunikationssektor gibt es in § 109 TKG eine Spezialregelung zu sogenannten technischen Schutzmaßnahmen. Danach hat jeder Dienstanbieter im Sinne des TKG angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogene Daten sowie der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen (§ 109 Abs. 1 TKG). Soweit es um den Betrieb von Telekommunikationsanlagen geht, sieht § 109 Abs. 2 und Abs. 3 TKG unter weiteren Voraussetzungen weitere spezielle Vorgaben vor. Hierzu gehören insbesondere die Erstellung eines Sicherheitskonzeptes sowie die Bestellung eines Sicherheitsbeauftragten.

In weiteren Gesetzen sind spezielle Vorgaben für die IT-Sicherheit vorgesehen. Auf diese wird hier zunächst nicht weiter eingegangen, da sie typischerweise nicht einschlägig sind im vorliegenden Kontext.

3.1.6 Rechte der Betroffenen

Der Betroffene hat in Österreich das Recht auf Auskunft. Auf Verlangen ist ihm innerhalb von 8 Wochen unentgeltlich Auskunft über die zu einer Person verarbeiteten Daten zu erteilen (§ 26 DSG 2000).

---

[1] Vgl. "Österreichisches Informationssicherheitshandbuch" Teil1 + Teil2, 2007 abrufbar auf http://demo.a-sit.at/siha-home/home/#teil_I.

Der Betroffene hat weiters das Recht auf Richtigstellung oder Löschung der Daten. Jedenfalls sind die Daten aber zu löschen, wenn sie für den Zweck der Datenanwendung nicht mehr benötigt werden (§ 27 DSG 2009). Ein Antrag ist dafür binnen 8 Wochen zu stellen. Löschen der Daten heißt dabei, dass der Datensatz vollkommen gelöscht werden muss (auch Backup Dateien).

Der Benutzer kann das Widerspruchsrecht geltend machen, wenn die Verwendung der Daten nicht gesetzlich vorgesehen ist. In diesem Fall hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen. Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datenanwendung kann der Betroffene jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Die Daten sind binnen acht Wochen zu löschen (vgl. § 28 DSG 2000)

In Deutschland sind die Rechte der Betroffenen in § 33 (Benachrichtigung des Betroffenen), § 34 (Auskunft an den Betroffenen) und § 35 (Berichtigung, Löschung und Sperrung von Daten) BDSG geregelt. Während die Benachrichtigung eine proaktive Pflicht der verantwortlichen Stelle ist, bestehen die Auskunftspflichten nach § 34 BDSG nur auf Aufforderung des Betroffenen. Zu berücksichtigen ist jedoch, dass durch die BDSG-Novelle zum 01.04.2010 eine Erweiterung der Auskunftspflicht durch eine Dokumentationspflicht erfolgt. § 35 BDSG regelt insbesondere die Löschung. Hierin kommt neben den speziellen Ausprägungen der Löschpflicht der allgemeine Grundsatz des BDSG zum Ausdruck, dass personenbezogene Daten zu löschen sind, wenn sie nicht mehr für ihren Verwendungszweck erforderlich sind.

Durch § 6 BDSG wird festgelegt, dass die Rechte des Betroffenen auf Auskunft und auf Berichtigung, Löschung oder Sperrung nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können.

3.1.7 Auftragsdatenverarbeitung

Das deutsche Datenschutzrecht sieht mit dem Institut der sogenannten Datenverarbeitung im Auftrag bzw. Auftragsdatenverarbeitung eine gesetzlich privilegierte Auslagerung von Tätigkeiten auf Dritte vor. Obgleich es sich bei dem beauftragten Unternehmen um ein von der verantwortlichen Stelle verschiedenes Unternehmen handelt, wird dieses auf Grund einer gesetzlichen Fiktion nach § 3 Abs. 8 BDSG nicht als Dritter im Sinne des Datenschutzrechts behandelt. In der Konsequenz liegt es, dass die Übertragung der Daten an dieses Unternehmen nicht die gesetzlichen Voraussetzungen einer Übermittlung erfüllen muss.

Voraussetzung für eine solche Auftragsdatenverarbeitung ist zusammengefasst, dass das andere Unternehmen als strikt weisungsgebundener Auftragnehmer (verlängerter Arm des Auftraggebers) tätig wird; eine Entscheidungsbefugnis in Bezug auf die Erhebung und Verwendung personenbezogener Daten darf dem

Auftragnehmer nicht zustehen. Des Weiteren muss ein schriftlicher Vertrag zwischen dem Auftraggeber und Auftragnehmer geschlossen werden, der den Anforderungen des § 11 BDSG genügt.

Die Auftragsdatenverarbeitung entbindet jedoch den Auftraggeber nicht von seinen datenschutzrechtlichen Pflichten. Der Auftraggeber ist im Außenverhältnis zu den Betroffenen allein und primär verantwortlich. Des Weiteren gelten für den Auftraggeber – obgleich die Auftragsausführung durch den Auftragsnehmer erfolgt – den oben dargestellten Grundsätzen des Datenschutzrechts. Insofern erfolgt keine Befreiung von Beschränkungen.

Darüber hinaus ist zu berücksichtigen, dass nach § 8 Abs. 3 BDSG die Privilegierung durch die Auftragsdatenverarbeitung nur gilt, wenn der Auftragnehmer seinen Sitz in der europäischen Union hat oder in einem Staat des EWR.

In Österreich besteht das Institut der „Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen (vgl. § 10 DSG 2000) Danach dürfen Auftraggeber bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hierfür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen. Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle unterliegt, ist der Datenschutzkommission mitzuteilen, es sei denn, dass die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht.

Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber eine Reihe gesetzlich normierter Pflichten. Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der Pflichten sind zum Zweck der Beweissicherung immer schriftlich festzuhalten. (vgl. § 11 Abs. 1 Z 1 bis 6 und § 11 Abs. 2 DSG 2000).

3.1.8 Zulässigkeit der Datenverwendung nach deutschem Recht

Die Zulässigkeit der Datenverwendung ist durch das deutsche Datenschutzrecht grundsätzlich in Form einer Zweiteilung geregelt: Die Erhebung und Verwendung kann auf der Grundlage und entsprechend der Reichweite einer Einwilligung erfolgen. Nach dem deutschen Verständnis des Datenschutzrechts kann der Betroffene grundsätzlich jede Erhebung und Verwendung seiner personenbezogenen Daten durch eine Einwilligung zulässig machen, da das Datenschutzrecht ein Ausfluss des grundrechtlich geschützten informationellen Selbstbestimmungsrechts ist. Gleichwohl sieht das Datenschutzrecht sowie die Rechtsprechung hierzu Schranken vor, wonach bestimmte Verarbeitungen einer Einwilligung nicht oder nicht ohne weiteres zugänglich sind. Namentlich ist zu

berücksichtigen, dass die Rechtsprechung des Bundesarbeitsgerichts die Freiwilligkeit von Einwilligungen durch Arbeitnehmer gegenüber ihren Arbeitgebern sehr kritisch prüft. Neben der Einwilligung kommen sogenannte gesetzliche Zulässigkeitstatbestände in Betracht. In § 95ff. TKG sowie § 14ff. TMG sind spezielle gesetzliche Zulässigkeitsregelungen für den Umgang mit Bestands- und Verkehrs-/Nutzungsdaten vorgesehen. Daneben sieht das BDSG in §§ 28, 29 BDSG gesetzliche Zulässigkeitstatbestände vor, die – anders als die Bestimmungen des TKG und des TMG – dadurch gekennzeichnet sind, dass sich die Zulässigkeit einer Erhebung und Verwendung personenbezogener Daten aus einer Abwägung der berechtigten Interesse der verantwortlichen Stelle mit den schutzwürdigen Interessen des Betroffenen ergeben können.

3.1.9 Exkurs: Arbeitnehmerrechte

In Österreich ist die Rechtslage im Bereich des arbeitnehmerrechtlichen Datenschutzes unübersichtlich. Die Rechtsfragen sind vielfältig und kaum übersehbar. Es zeigt sich jedenfalls, dass die österreichische Rechtsordnung im Hinblick auf den Arbeitnehmerdatenschutz unterdeterminiert ist. Der Schutz personenbezogener Informationen ist jedenfalls immer nur im konkreten Sachzusammenhang und unter Berücksichtigung grundlegender arbeitsrechtlicher Strukturen zu erfassen ist. Betriebsverfassungsrechtlich ist zu beachten, dass verschiedene automationsunterstützte Ermittlungen der Zustimmung des Betriebsrates bedürfen (vgl. Art 96 und 96 a ArbVG).[2]

In Deutschland existierte bis zum 01.09.2009 keine explizite gesetzliche Regelung zum Arbeitnehmerdatenschutz. Vielmehr wurde der Persönlichkeitsschutz der Arbeitnehmer durch arbeitsrechtliche Bestimmungen geregelt. Als allgemeine arbeitsrechtliche Datenschutznorm in diesem Sinne ließe sich § 83 Betriebsverfassungsgesetz (BetrVG) nennen, wobei diese Vorschrift sich allerdings zu Zulässigkeitsfragen nicht äußert, sondern lediglich ein spezielles Informations- und Korrekturrecht gewährt. Es ist daher hinsichtlich der Zulässigkeit der Verarbeitung auf den Anspruch des Beschäftigten auf Persönlichkeitsrechtsschutz (vgl. § 75 Abs. 2 BetrVG) und die Wahrung seiner Intimsphäre abgestellt worden. Obgleich das BDSG auch auf das Verhältnis des Arbeitnehmers zu seinem Arbeitgeber Anwendung findet, hat das Bundesarbeitsgericht (BAG) seit 1984 unter Berufung auf das Volkszählungsurteil recht eigenständig einen Schutz des informationellen Selbstbestimmungsrechts des Arbeitnehmers entwickelt. In seiner Rechtsprechung prüft das BAG die Frage der Verletzung des allgemeinen Persönlichkeitsrechts bzw. das Recht auf informationelle Selbstbestimmung des Arbeitnehmers stets im Rahmen einer Güter- und Interessensabwägung unter Beachtung des Verhältnismäßigkeitsprinzips. Das BAG leitet hieraus recht eigenständig Richtlinien ab, ohne strikt auf die Bestimmungen des BDSG Bezug zu

[2] Vgl. im Detail die relevanten Bestimmungen und ein Literaturliste unter http://www.univie.ac.at/zib/pdf/Brodil_Lehrveranstaltungsunterlage.pdf).

nehmen. Im Ergebnis ist jedoch eine Parallelität des Vorgehens des BAG im Rahmen der Güter- und Interessensabwägung unter Beachtung des Verhältnismäßigkeitsprinzips und der nach § 28 BDSG anzustellenden Interessenabwägung zu erkennen. Zu beachten ist allerdings, dass das BAG anders als § 28 BDSG der besonderen Interessenslage des Arbeitnehmers im Verhältnis zu seinem Arbeitgeber Rechnung trägt. Diese Überlagerung wird besonders deutlich bei der Bewertung der Einwilligung des Arbeitnehmers in die Verarbeitung auf ihn bezogener Daten. Denn dort ist in der Rechtsprechung der Arbeitsgerichte erkennbar, dass sie der Situation Rechnung tragen, dass eine Einwilligung eines Arbeitnehmers gegenüber seinem Arbeitgeber in der Praxis nur eingeschränkt unabhängig getroffen werden kann.

Vor dem Hintergrund des Datenschutzskandals bei der Bahn AG wegen der „Bespitzelung von Mitarbeitern zur Korruptionsbekämpfung“ wurde im Rahmen einer Datenschutz-Novelle zum 01.09.2009 in Deutschland durch § 32 BDSG eine Regelung zum Beschäftigtendatenschutz eingeführt. Wer als Beschäftigter geschützt ist, ergibt sich aus § 3 Abs. 11 BDSG. Die Zulässigkeitsregelung in § 32 BDSG ist im Wesentlichen zweigeteilt:

- § 32 Abs. 1 S. 1 BDSG regelt die Erhebung und Verwendung von personenbezogenen Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses. Diese ist zulässig, wenn sie für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Im praktischen Ergebnis ist diese Regelung an die bereits bisher erfolgende Interessensabwägung angelehnt.
- § 32 Abs. 1 S. 2 BDSG regelt die Erhebung und Verwendung von personenbezogenen Daten eines Beschäftigten zur Aufdeckung von Straftaten und knüpft die Zulässigkeit in diesem Spezialfall an weitere Voraussetzungen.

Die Datenbestimmungen des TKG und des TMG kommen im Dienst- und Arbeitsverhältnis nicht zur Anwendung, soweit die Bereitstellung der Telekommunikation und / oder Telemedien zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt. Dasselbe gilt für den Schutz durch das Fernmeldegeheimnis. Für die Anwendung dieser Bestimmungen kann daher in der Praxis entscheidend sein, ob den Mitarbeitern die Privatnutzung der Einrichtungen gestattet ist bzw. diese geduldet wird.

3.1.10 EU-Hintergrund

Für den modernen Datenschutz in den Mitgliedsstaaten der Europäischen Union ist die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr die entscheidende Grundlage.

Ergänzend regelt die Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15.12.1997 über die Verarbeitung personenbezogener Daten und der Schutz der Privatsphäre im Bereich der Telekommunikation – sogenannte ISDN-Datenschutzrichtlinie – Spezialfragen des Datenschutzes im Bereich der Telekommunikation. Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.06.2002 über die Verarbeitung personenbezogener Daten und der Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) regelt Spezialfragen des Datenschutzes und passt die Richtlinie 97/66/EG an die Entwicklung der Märkte und Technologien für elektronische Kommunikationsdienste an, um den Nutzern öffentlich zugänglicher elektronischer Kommunikationsdienste unabhängig von der zugrundeliegenden Technologie den gleichen Grad des Schutzes personenbezogener Daten und der Privatsphäre zu bieten. Die Richtlinie 97/66/EG ist daher durch die Richtlinie 2002/58/EG aufgehoben worden (Erwägungsgrund 4 der Richtlinie 2002/58/EG).

Die Richtlinien des Europäischen Parlaments und des Rates haben in den Mitgliedsstaaten grundsätzlich keine unmittelbare Wirkung. Sie müssen jeweils durch ein nationales Gesetz in dem jeweiligen Mitgliedsstaat umgesetzt und dadurch zur Anwendung gebracht werden, was in Österreich durch das DSG 2000 und in Deutschland durch das BDSG erfolgt ist.

3.1.11 Exkurs: Geodatenrichtlinie

Die Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14.03.2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) hat zum Ziel, allgemeine Bestimmungen für die Schaffung der Geodateninfrastruktur in der Europäischen Gemeinschaft (abgekürzt als „INSPIRE“) für die Zwecke der gemeinschaftlichen Umweltpolitik sowie andere politischer Maßnahmen oder sonstige Tätigkeiten, die Auswirkung auf die Umwelt haben können, zu erlassen.

Ziele der INSPIRE-Richtlinie sind insbesondere die Verbesserung der Verfügbarkeit, Qualität, Organisation, Zugänglichkeit und Nutzung von Geodaten durch andere (von der die Verfügungsrechte über die Geodaten besitzenden öffentlichen Geodatenstelle verschiedenen) öffentliche Stellen oder die Öffentlichkeit. Dadurch soll vor allem die Einbeziehung der Erfordernisse des Umweltschutzes in den Gemeinschaftspolitiken im Sinne einer integralen Umweltpolitik verbessert und durch die transparentere Nutzbarkeit der Geodaten für die Bürger, Wissenschaft, Wirtschaft und Verwaltung das Wertschöpfungspotential der Geodaten weiter aktiviert werden können.

In Österreich wurde die Richtlinie am 2. März 2010 ist mit BGBl. I Nr. 14/2010, dem BG über eine umweltrelevante Geodateninfrastrukturgesetz des Bundes (Geodateninfrastrukturgesetz - GeoDIG) umgesetzt.

In Deutschland wurde die Richtlinie mit dem Geodatenzugangsgesetz vom 10.02.2009 (GeoZG) umgesetzt. Dieses Gesetz dient dem Aufbau einer nationalen Geodateninfrastruktur. Es schafft den rechtlichen Rahmen für den Zugang zu

Geodaten, Geodatendiensten und Metadaten von geodatenhaltenden Stellen sowie die Nutzung dieser Daten und Dienste, insbesondere für Maßnahmen, die Auswirkung auf die Umwelt haben können (vgl. § 1 GeoZG).

Die Richtlinie sowie das nationale Umsetzungsgesetz sind nicht primär datenschutzrechtliche Bestimmungen, sondern dienen dem Zugang zu entsprechenden Informationen. Auf die Bestimmungen der Richtlinie und der nationalen Umsetzungsgesetze wird nachfolgend – soweit im Rahmen der Projekte geboten – eingegangen.

3.1.12 Exkurs: Neuerungen im österreichischen DSG

Das DSG 2000 wurde im Jahr 2010 novelliert. Die wesentlichen Änderungen betreffen

- die Videoüberwachung
- das Registrierungsverfahren (neu)
- die Stärkung der Befugnis für die Datenschutzkommission
- die Straffung des Beschwerdeverfahrens vor der DSK

Ziel des Registrierungsverfahren (neu) ist es, bei unproblematischen Meldungen eine Vereinfachung herbeizuführen und die Ressourcen der Datenschutzkommission verstärkt dort einzusetzen, wo Geheimhaltungsinteressen ernsthaft bedroht sind. Dazu wird ein Online-Registrierungsverfahren für nicht vorab kontrollpflichtige Datenanwendungen eingeführt und ein massiver Ausbau der Befugnis der Datenschutzkommission dort eingeführt, wo sich Probleme bei registrierten Datenschutzanwendungen ergeben. Die Datenschutzkommission wurde insofern gestärkt und zu einer Art Datenschutzpolizei ausgebaut, insofern gerade besonders gefährliche Datenschutzanwendungen, die nicht registriert, jederzeit untersagt werden können, wenn eine wesentliche und unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen (vgl. § 30 Abs. 6a DSG 2000).

Auf die Änderung im Bereich der Videoüberwachung wird im folgenden Exkurs eingegangen.

3.1.13 Exkurs: Videoüberwachung

Die Videoüberwachung wurde durch die Novelle zum DSG 2000 nun erstmals gesondert geregelt. Der Gesetzgeber folgte insofern dem Beispiel Deutschland (§ 6b BDSG).[3]

[3] „Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies

Videoüberwachung ist gemäß § 50a DSG 2000 die systematische, fortlaufende Feststellung von Ereignissen in Bezug auf ein bestimmtes Objekt, eine bestimmte Person durch technische Bildaufnahme oder Bildübertragungsgeräte. § 6f DSG 2000 ist einzuhalten, insbesondere der Verhältnismäßigkeitsgrundsatz im Sinne des Einsatzes des gelindesten Mittels. Es müssen ein rechtmäßiger Zweck im Sinne eines Schutzes und die Erfüllung rechtlicher Sorgfaltspflichten inklusive Beweissicherung vorliegen und es dürfen keine schutzwürdigen Geheimhaltungsinteressen verletzt sein.

Wesentlich ist, dass die Videoüberwachung auf zwei Zwecke beschränkt ist, nämlich dem Schutz des überwachten Objekts oder der überwachten Person bzw. die Erfüllung von rechtlichen Sorgfaltspflichten (zum Beispiel § 1319a ABGB, § 19 EisBG, etc.). Die Novelle normiert explizit die Verbote überschießender Einsatzmöglichkeiten von Videoüberwachung im höchstpersönlichen Lebensbereich, Mitarbeiterkontrolle zum elektronischen Abgleich mit anderen Bilddaten und die Durchsuchung nach sensiblen Daten.

Es besteht eine durchgängige Vorabkontrollpflicht mit Ausnahme für deutlich herabgesetzte Gefährdungspotentiale. Es besteht weiters eine durchgängige Protokollierungspflicht ausgenommen bei der Echtzeitüberwachung, weil dort keine Daten gespeichert werden. Es besteht zuletzt eine Erlöschungspflicht nach spätestens 72 Stunden, Ausnahmen gibt es nur im begründeten Einzelfall.

Im Bereich der Videoüberwachung besteht eine strenge Kennzeichnungspflicht und ein spezielles Auskunftsrecht, dass grundsätzlich die Übersendung einer kopierten Aufnahme beinhaltet.

Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen verletzt, wenn 1. diese im lebenswichtigen Interesse einer Person erfolgt, oder 2. Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder 3. er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.

Ein Betroffener ist durch eine Videoüberwachung ausschließlich dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen verletzt, wenn sie nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt und 1. bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder 2. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der

---

zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen."

überwachten Person auferlegen, oder 3. sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 bis 4 hinaus in folgenden Fällen übermittelt werden: 1. an die zuständige Behörde oder das zuständige Gericht, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder 2. an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, eingeräumten Befugnisse, auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt oder die überwachte Person richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.

Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren. Aufgezeichnete Daten sind, sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder für Zwecke nach § 50a Abs. 6 benötigt werden, spätestens nach 72 Stunden zu löschen. Eine beabsichtigte längere Aufbewahrungsdauer ist in der Meldung anzuführen und zu begründen. In diesem Fall darf die Datenschutzkommission die Videoüberwachung nur registrieren, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist.

Videoüberwachungen unterliegen der Meldepflicht. Sofern der Auftraggeber nicht in der Meldung zusagt, die Videoüberwachungsdaten zu verschlüsseln und unter Hinterlegung des einzigen Schlüssels bei der Datenschutzkommission sicherzustellen, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet, unterliegen sie der Vorabkontrolle.

Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Auftraggeber eindeutig hervorzugehen, es sei denn, dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen. Keine Kennzeichnungsverpflichtung besteht bei Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

3.2 Immaterialgüterrechte

Innovationen können im vorliegenden Kontext vor allem unter zwei Aspekten geschützt sein:

- Patentrecht
- Urheberrecht

Wobei in Bezug auf dieselbe „Innovation“ typischerweise nur das eine oder das andere zur Anwendung kommen. Sie unterscheiden sich in ihren Voraussetzungen und in ihrer Schutzwirkung.

3.2.1 Patentrecht

Das Patentrecht ist ein geprüftes formelles Schutzrecht. Zu seiner Erlangung gibt es verschiedene Möglichkeiten: ein nationales Patent nach den Vorschriften des (österreichischen oder deutschen) Patentgesetzes, ein europäisches Patent nach den Regeln des europäischen Patentübereinkommens oder internationale Anmeldung entsprechend dem Patentzusammenarbeitsvertrag (PCT), wobei dieses internationale Verfahren der Vereinfachung der Anmeldung dient und in ein nationales Patenterteilungsverfahren mündet.

Patente werden für Erfindungen auf allen Gebieten der Technik erteilt, sofern sie neu sind, sich für den Fachmann nicht in nahe liegender Weise aus dem Stand der Technik ergeben (bzw. auf einer erfinderischen Tätigkeit beruhen (§ 1 Abs. 1 dt. PatG) und gewerblich anwendbar sind (§ 1 Abs1 öst. Patentgesetz). Als Erfindungen in diesem Sinn werden insbesondere nicht angesehen: Entdeckungen sowie wissenschaftliche Theorien und mathematische Methoden, ästhetische Formschöpfungen, Pläne, Regeln und Verfahren für gedankliche Tätigkeiten, für Spiele oder für geschäftliche Tätigkeiten sowie Programme für Datenverarbeitungsanlagen und die Wiedergabe von Informationen , wobei dies nur soweit gilt, als für die genannten Gegenstände oder Tätigkeiten als solche Schutz begehrt wird (§ 1 Abs. 3 öst. PatentG; ebenso das dt. PatG).

Das entscheidende Abgrenzungsmerkmal zu anderen Leistungsschutzrechten ist die Technizität. Eine Erfindung ist eine Lehre zum technischen Handeln, mit der ein technisches Problem – auch als Aufgabe bezeichnet – gelöst wird. Nach st. Rspr. des dt. Bundesgerichtshofs (BGH) wird eine Lehre als technisch bezeichnet, wenn sie sich unmittelbar zur Erreichung eines kausal übersehbaren Erfolges des Einsatzes beherrschbarer Naturkräfte außerhalb der menschlichen Verstandestätigkeit bedient. Was hierunter zu verstehen ist, ist nicht starr festgelegt, sondern ist Modifikationen zugänglich, wie die Rechtsprechung des BGH gezeigt hat.

Eine weitere entscheidende Voraussetzung ist, dass die Erfindung neu ist. Eine Erfindung gilt als neu, wenn sie nicht zum Stand der Technik gehört. Der Stand der Technik umfasst alle Kenntnisse, die vor dem für den Zeitrang der Anmeldung maßgeblichen Tag durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise der Öffentlichkeit zugänglich gemacht worden sind (§ 3

Abs. 1 öst. PatentG; ebenso im dt. PatG). Das öst. PatentG und das dt. PatG enthalten zur Bewertung der Neuheit weitere Konkretisierungen dieses Grundsatzes.

Voraussetzung für den rechtlichen Schutz ist die Anmeldung und die Erteilung eines Patents. Die Anmeldung muss bei einer zuständigen Behörde angemeldet erfolgen. Diese prüft die Erfindung auf ihre Patentfähigkeit erteilt dann gegebenenfalls das Patent. Im Rahmen der Patentanmeldung ist die Erfindung so deutlich und vollständig zu offenbaren, dass ein Fachmann sie ausführen kann. Aufgrund dieser Pflicht zur Offenbarung wird es von Erfindern oftmals vorgezogen, kein Patent anzumelden sondern die „Funktionsweise“ der Erfindung tatsächlich geheim zu halten.

Das Patentrecht unterscheidet zwischen dem Recht an der Erfindung, dem Recht auf das Patent und dem Recht aus dem Patent. Das Recht an der Erfindung sowie das Recht auf das Patent stehen dem Erfinder, damit also einer natürlichen Person, welche die Erfindung gemacht hat, zu. Das Recht an der Erfindung entsteht als Realakt mit ihrer Verlautbarung. Das ist jede Kundgebung der Erfindung an die Außenwelt nach Beendigung des Schöpfungsaktes. Dieses Recht an der Erfindung endet mit ihrer Veröffentlichung. Das Recht auf das Patent endet mit der Patenterteilung. Das Recht aus dem Patent hat derjenige, dem das Patent durch die zuständige Behörde erteilt wird. Für die Rechtsdurchsetzung gegenüber Dritten ist dieses Recht aus dem Patent entscheidend.

Macht ein Arbeitnehmer im privaten oder öffentlichen Dienst während der Dauer des Arbeits- oder Dienstverhältnisses eine Erfindung, so liegt eine sogenannte Diensterfindung vor. Dies ist eine Erfindung, die aufgrund der dem Arbeitnehmer obliegenden Tätigkeiten entstanden ist oder maßgeblich auf Erfahrung des Betriebes beruhen. Alle anderen Erfindungen sind hingegen sogenannte freie Erfindungen. Nach österreichischem und deutschem Recht müssen sogenannte Diensterfindungen dem Arbeitgeber unverzüglich schriftlich gemeldet werden. Der Arbeitgeber hat sich sodann innerhalb einer Frist von vier Monaten zu erklären, ob er die Erfindung unbeschränkt oder beschränkt in Anspruch nehmen will. Will er sie unbeschränkt in Anspruch nehmen, geht das Recht an der Erfindung auf ihn über. Will er das Recht nur beschränkt in Anspruch nehmen, erwirbt er ein einfaches Nutzungsrecht. Als Gegenleistung erhält der Arbeitnehmer eine angemessene Vergütung. Diese kann entweder vertraglich festgelegt werden oder muss nach einem komplizierten Schlüssel berechnet werden. Falls eine Diensterfindung nicht oder nur beschränkt in Anspruch genommen wird oder vom Arbeitgeber wieder freigegeben wird, kann diese von dem Arbeitnehmer anderweitig verwertet werden. (vgl. § 6 öst. PatentG)

Das Patent vermittelt für die Dauer von 20 Jahren nach dem Tag der Anmeldung Schutz (§ 28 öst. PatentG; § 16 dt. PatG). Das Patent kann auch früher – beispielsweise durch Verzicht oder mangelnde Gebührenzahlung – enden (§ 28 Abs. 2 öst. PatentG; § 20 Abs. 1 PatG). Mit Rückwirkung kann der Patentschutz durch einen Widerruf des Patents oder die Nichtigerklärung des Patents entzogen werden.

Das erteilte Patent gewährt seinem Inhaber das ausschließliche Recht, die patentierte Erfindung zu benutzen und jedem zu verbieten,

- das Erzeugnis, das Gegenstand des Patents ist, herzustellen, anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu diesem Zweck entweder einzuführen oder zu besitzen,
- ein Verfahren, das Gegenstandes des Patents ist, anzuwenden oder seine Anwendung anzubieten, wenn der Anbieter bösgläubig ist,
- das durch ein Verfahren, das Gegenstand des Patent ist, unmittelbar hergestellte Erzeugnis anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu diesem Zweck entweder einzuführen oder zu besitzen oder,
- anderen als zur Benutzung der patentierten Erfindung berechtigten Person Mittel die sich auf ein wesentliches Element der Erfindung beziehen, zur Benutzung der Erfindung anzubieten oder zu liefern, wenn der Dritte weiß oder es offensichtlich ist, dass diese Mittel geeignet und bestimmt sind, für die Benutzung der Erfindung verwendet zu werden (§ 22 öst. PatentG; § 9 S. 2, 10 Abs. 1 dt. PatG).

Der Schutzumfang des Patents bestimmt sich nach den in der Patentschrift formulierten Patentansprüchen (§ 31 öst. PatentG; § 14 dt. PatG). Zur Bestimmung eines Verletzungsfalls wird der so beschriebene Schutzbereich mit dem Verletzungsgegenstand verglichen. Eine Verletzung kann auch dann vorliegen, wenn einzelne Merkmale des Patents durch andere ausgetauscht werden, soweit weitere Voraussetzungen vorliegen.

3.2.2 Urheberrecht

Das Urheberecht ist kein formelles und kein geprüftes Schutzrecht. Es entsteht automatisch kraft Gesetzes durch die Schaffung eines geschützten Werkes in der Hand seines Schöpfers. Das bedeutet insbesondere, dass es keiner Anmeldung des Urheberechts bedarf und dementsprechend auch keine Erteilung eines Urheberrechts erfolgt.

Welche Werke urheberechtlich geschützt sein können, wird in § 2 ff Urheberrechtsgesetz (UrhG) beispielhaft aufgezählt (die Rechtslage ist in Österreich und Deutschland weitgehend identisch). Zu den dort genannten gehören beispielsweise auch Computerprogramme, für die in § 40a ff. UrhG spezielle Regelungen vorgesehen sind. Darüber hinaus enthält das Urheberrecht in § 40f UrhG auch Spezialregelungen zum Schutz des Datenbankherstellers; aufgrund seiner Ausgestaltung ist der Schutz des Datenbankherstellers in gewisser Weise ein Fremdkörper im Urheberrecht.

Die zu erfüllenden Schutzvoraussetzungen werden in § 1 Abs. 1 UrhG wie folgt beschrieben: „*Werke im Sinne dieses Gesetzes sind eigentümliche geistige Schöpfungen auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste und der Filmkunst*“. Das zu schützende Werk muss also von einem Menschen stammen und individuell sein. Die Individualität ist zu bejahen, wenn das Werk sich

nicht in der bloßen Wiedergabe von Vorbekanntem Allgemein- oder Fremdgut und in der Anwendung bekannter Methoden oder Konzeptionen erschöpft. Unter diesem Aspekt kann auch ein sogenanntes Datenbankwerk – zu unterscheiden von der einfachen Datenbank – als ein Sammelwerk, dessen Element die systematische oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf anderer Weise zugänglich sind (§ 40f UrhG), geschützt sein. Ein zur Schaffung des Datenbankwerks oder zur Ermöglichung des Zugangs zu dessen Elementen verwendetes Computerprogramms (vgl. § 40 f Abs. 1 UrhG) ist nicht Bestandteil des Datenbankwerkes. Vorausgesetzt wird für den Urheberrechtschutz im Allgemeinen ein Schaffungsvorgang, der eine gewisse Gestaltungshöhe, bzw. einen gewissen Qualitätsgehalt besitzt. Entscheidend für den urheberrechtlichen Schutz ist, dass die konkrete Darstellung bzw. Ausdrucksform geschützt ist. Nicht hingegen geschützt ist die hinter dieser Darstellung stehende bloße Idee oder das Konzept.

Schöpfer des Werkes ist derjenige, der die persönliche geistige Schöpfung tatsächlich erbracht hat. Das können nur natürliche Personen sein; nicht aber der Ideengeber oder der Auftraggeber des Werkes. Das gilt auch für das sogenannte Datenbankwerk im Sinne des § 40f UrhG. Für den Schutz der Datenbank nach deutschem Urheberrecht (vgl. § 87a ff. UrhG) gilt dies hingegen nicht. Dort ist derjenige geschützt, der die wesentliche Investition tätigt. Eine inhaltlich vergleichbare Regelung enthält § 76d öst UrhR:

„Wer die Investition im Sinne des § 76c vorgenommen hat (Hersteller), hat mit den vom Gesetz bestimmten Beschränkungen das ausschließliche Recht, die ganze Datenbank oder einen nach Art oder Umfang wesentlichen Teil derselben zu vervielfältigen, zu verbreiten, durch Rundfunk zu senden, öffentlich wiederzugeben und der Öffentlichkeit zur Verfügung zu stellen. Diesen Verwertungshandlungen stehen die wiederholte und systematische Vervielfältigung, Verbreitung, Rundfunksendung und öffentliche Wiedergabe von unwesentlichen Teilen der Datenbank gleich, wenn diese Handlungen der normalen Verwertung der Datenbank entgegenstehen oder die berechtigten Interessen des Herstellers der Datenbank unzumutbar beeinträchtigen.“

Für den Datenbankschutz ist nach deutschem Recht (vgl. § 87a ff. UrhG) anders als nach österreichischem Recht auch keine geistige Schöpfungshöhe erforderlich.

Nach § 12 UrhG (vgl. in Deutschland § 10 UrhG) wird vermutet, dass derjenige, der auf einem Werkstück als Urheber bezeichnet ist, auch dessen Schöpfer ist. Für die Urheberrechte gilt, dass die 70jährige Schutzfrist mit Ablauf des Tages beginnt, an dem der Urheber stirbt (§ 60UrhG). Mit Ablauf der Schutzfrist wird das Werk sogenannt gemeinfrei. Das bedeutet, es kann von jedermann ungehindert genutzt werden.

In Bezug auf den Schutz durch das Urheberrecht muss zwischen den sogenannten persönlichkeitsrechtlichen Befugnissen und den sogenannten Verwertungsrechten unterschieden werden. Das Urheberrecht ist ein Ausfluss der Menschenwürde. Dementsprechend gibt es urheberrechtliche Ansprüche, die stets nur dem Urheber zustehen (beispielsweise das Namensnennungsrecht). Diese

Urheberpersönlichkeitsrechte können nicht veräußert werden; sie können jedoch in gewissen Umfängen vertraglich eingeschränkt werden. Davon zu unterscheiden sind die sogenannten Verwertungsrechte. Diese kann der Urheber auf Dritte übertragen. Dies kann er als ausschließliche Rechtsübertragung vornehmen, so dass nur dieser Dritte berechtigt ist, oder als einfache Rechtsübertragung, so dass zwar der Dritte berechtigt ist, aber auch weitere Dritte, sofern ihnen der Urheber dieses Recht einräumt.

Das Recht zur körperlichen Verwertung umfasst insbesondere das Vervielfältigungsrecht, das Verbreitungsrecht und das Ausstellungsrecht. Der Urheber hat ferner das Recht, sein Werk in unkörperlicher Form öffentlich wiederzugeben (Recht der öffentlichen Wiedergabe). Das Recht der öffentlichen Wiedergabe umfasst insbesondere das Recht der öffentlichen Zugänglichmachung, das Senderecht, das Recht der Wiedergabe durch Bild- oder Tonträger.

Die Bearbeitung oder andere Umgestaltungen des Werks dürfen nur mit Einwilligung des Urhebers des bearbeitenden oder umgestaltenden Werks veröffentlicht oder verwertet werden. Das bedeutet, dass auch bei der „Fortsetzung“ eines geschützten Werks Rechte eingeholt werden müssen.

§ 27 UrhG enthält spezielle Regelungen zur Übertragung von Verwertungsrechten. Die Besonderheit ist dabei, dass das Urheberrecht im Zweifelsfall den Vorrang dem Schutz des Urhebers einräumt. Bei einer vertraglich nicht eindeutig geregelten Sachlage erhält der Rechteerwerber nur die Rechte, die zwingend entsprechend dem Vertragszweck erforderlich sind und im Zweifel verbleiben die übrigen Rechte beim Urheber.

Für Dienstnehmer, die Computerprogramme schaffen besteht eine Sonderregelung in § 40b: Wird ein Computerprogramm von einem Dienstnehmer in Erfüllung seiner dienstlichen Obliegenheiten geschaffen, so steht dem Dienstgeber hieran ein unbeschränktes Werknutzungsrecht zu, wenn er mit dem Urheber nichts anderes vereinbart hat. In solchen Fällen ist der Dienstgeber auch zur Ausübung der in § 20 und § 21 Abs. 1 bezeichneten Rechte berechtigt; das Recht des Urhebers, nach § 19 die Urheberschaft für sich in Anspruch zu nehmen, bleibt unberührt.

3.3 Vertragsrechtliche Aspekte

Verkehrstelematikprojekte werden sich in der überwiegenden Zahl der Fälle in unterschiedlicher Ausgestaltung mit der Beschaffung / Generierung, Aufbereitung und dem Vertrieb / der Verwertung von Informationen (Daten) befassen. In diesen einzelnen Projektphasen werden jeweils über die Leistungserbringung, insbesondere über die Beschaffung von Daten und deren Vertrieb – Verträge geschlossen.

Das österreichische ebenso wie das deutsche Zivilrecht typisiert verschiedene Vertragsarten und sieht für diese gesetzlich ausgestaltete Primärrechte (insbesondere Ansprüche auf Leistung und Gegenleistung) sowie Sekundärrechte (etwa Mängelhaftung) vor. Diese Vertragsarten sind in Österreich zu Beginn des 19. Jahrhunderts, in Deutschland zu Beginn des 20. Jahrhunderts festgelegt worden. Sie

sind aufgrund dessen nicht ohne weiteres in der Lage, den besonderen Interessen im Rahmen von komplexen Projekten im Jahr 21. Jahrhundert gerecht zu werden.

Die Leistung müsste etwa danach kategorisiert sein, ob der Vertragspartner nur eine Leistung erbringen soll, im Ergebnis einen Erfolg schuldet, oder einen Gegenstand nur zeitlich begrenzte Dauer oder auf unbegrenzte Zeit überlässt. Das ist bei Leistungsbeziehungen im Bereich der Telematik häufig überhaupt nicht möglich. Es muss daher durch, sehr detaillierte und fallspezifische vertragliche Regelungen ein Ausgleich der verschiedenen Interessen der Vertragsparteien unter Berücksichtigung des konkreten Sachverhalts und der besonderen Risiken stattfinden. Hierzu bedarf es expliziter vertraglicher Regelungen, das dispositive gesetzliche Zivilrecht wird als Rückfallslösung bei Fehlen einer vertraglichen Regelung oftmals nicht eindeutig sein oder keine Antwort geben. Verkehrstelematikprojekte bedürfen daher in der Regel einer sehr detaillierten Ausgestaltung.

Ein Vertrag gliedert sich typischerweise in eine Leistungsbeschreibung, welche die zu erbringende Leistung beschreibt und eine rechtliche Regelung dieser Leistungserbringung. Um dies an einem Beispiel zu verdeutlichen: Die Verfügbarkeit der Informationen und deren Qualität lassen sich nicht per se und auch nur selten – aufgrund der Innovationskraft der Projekte – anhand anderer Projekte bestimmen. Es muss daher zwischen den Parteien geklärt werden, welche Leistungsparameter die eine Partei wünscht und die andere bereit ist, zu vergüten. Hiervon ausgehend muss die Frage der Haftung zwischen den Parteien geklärt werden, falls es Abweichungen von der zugesagten Leistung geben sollte oder es zu Schäden aufgrund von Abweichungen von der zugesagten Leistung kommen sollte.

Nach dem bürgerlichen Recht gilt der Grundsatz der Vertragsfreiheit. Die Parteien können regeln, worauf immer sie sich gemeinsam verständigen. Diese Privatautonomie findet jedoch in einigen gesetzlichen Bestimmungen ihre Grenzen. Diese gesetzlichen Bestimmungen sehen Beschränkungen der Gestaltungsfreiheit meist zum Schutz einer der Parteien und zuweilen zum Schutz der Allgemeinheit vor. Ein typisches Beispiel hierfür sind die Bestimmungen des AGB-Rechts, die Beschränkungen für standardmäßig verwendete Vertragsregelungen vorsehen, weil sie den Verwender der AGB für den „mächtigeren“ Vertragspartner halten.

In jüngerer Vergangenheit sind auf der Grundlage der EU-Fernabsatzrichtlinie auch besondere Schutzbestimmungen im Bereich der Distanzgeschäfte – beispielsweise vermittels Telekommunikation – in Kraft getreten. Eine weiteres Beispiel hierfür sind spezielle Bestimmungen für Verbraucher-/Konsumentenschutz.

3.3.1 Leistungsbeschreibung (Quality of Service und Verfügbarkeit)

Im Bereich innovativer Telematikprojekte gibt es keinen Standard, der es ohne konkrete vertragliche Festlegung ermöglichen würde, zu bestimmen, welche Leistung zwischen den Parteien gewollt war. Es liegt daher im beiderseitigen Interesse, durch sehr genaue vertragliche Regelungen (Leistungsbeschreibung) festzulegen, welche Leistung der Anbieter erbringen wird und welche Leistungen damit der Abnehmer vergüten wird. Unklarheiten hierüber führen zu nicht unerheblichen Unsicherheiten in

den Rechtsfolgen. In Deutschland etwa hat die Rechtsprechung festgelegt, dass im Online-Bereich der Anbieter eine 100%ige Verfügbarkeit – beispielsweise eine Online-Banking-Plattform – schuldet, wenn eine abweichende Leistungsbeschreibung nicht erfolgt ist; vor dem Hintergrund dieser Rechtsprechung ist derzeit in Deutschland umstritten, ob überhaupt eine abweichende Regelung möglich ist.

Ebenso verhält es sich mit der sogenannten Quality of Service. Auch hier können die Leistungsbereitschaft und die Erwartungshaltung der Vertragsparteien erheblich auseinander fallen. Solange kein Vergleichsmaßstab – wie typischerweise bei innovativen Telematikprojekten – besteht, ist eine Bestimmung ohne exakte vertragliche Regelung nicht möglich.

3.3.2 Sekundärrechte

Aufgrund der Schwierigkeit bei der Einordnung der Projekte unter die typisierten Verträge des Bürgerlichen Rechts ist es dringend erforderlich, die Sekundärrechte – im Rahmen des gesetzlich zulässigen – eigenständig zu regeln, damit für beide Seiten erkennbare und klare Folgen bei mangelhafter Leistung auf der Hand liegen.

Im Bereich der innovativen Verkehrstelematikprojekte besteht für den Anbieter auch ein erhebliches wirtschaftliches Interesse daran, Risiken im Vertrag adäquat ausgleichen zu können. Ein solcher Ausgleich kann sinnvoll nur dadurch erfolgen, dass er sich mit dem Abnehmer der Leistungen auf bestimmte Haftungsregelungen verständigt. Dies dient beiden Seiten dazu die wirtschaftlichen Risiken kalkulieren zu können.

3.3.3 Lieferantenbeziehung

Im Rahmen von innovativen Verkehrstelematikprojekten wird der Anbieter häufig darauf angewiesen sein, Daten aus Drittquellen zu beschaffen. Er kann sich dabei auf gewerbliche Anbieter solcher Leistungen zurückgreifen, die Daten können aber auch von Verbrauchern stammen. Für den Anbieter ist es von erheblicher Bedeutung, auf dieser Vorleistungsebene zu klären, mit welcher Qualität und welcher Verfügbarkeit ihm Informationen geliefert werden. Hieraus ergeben sich nämlich maßgebliche Vorgaben für den Absatz seiner Leistungen, da er auch nur das absetzen kann, was er im Rahmen der Vorleistungen erhalten hat.

Es werden sich hier zwei unterschiedliche Konstellationen ergeben, je nachdem ob der Anbieter die gesamten Informationen von einem „Vorleistenden“ – beispielsweise einem Unternehmen – oder von einer Mehrzahl von „Vorleistenden“ – beispielsweise von Mobilfunknutzern als Verbraucher – erhalten wird. Im zuletzt genannten Fall wird er die vertraglichen Beziehungen auf der Grundlage von Standardverträgen regeln wollen. Bei der Ausgestaltung dieser Verträge sind beispielsweise die Vorgaben des AGB-Rechts zu berücksichtigen.

3.3.4 Vertrieb

Im Rahmen des Vertriebs des Telematikangebots ist aus rechtlicher Sicht eine grundlegende Unterscheidung danach erforderlich, ob die Abnehmer Gewerbetreibende oder Verbraucher sind. Weniger relevant hingegen ist, ob es sich um einen einzelnen oder um mehrere Abnehmer handelt.

3.3.4.1 Verbraucher/Konsumenten

Beim Absatz von Telematikinformationen an Verbraucher muss im Rahmen der vertraglichen Gestaltung neben dem AGB-Recht insbesondere das Konsumentenschutzrecht berücksichtigt werden. Hier können insbesondere die Regelungen über Fernabsatzverträge und Verträge im elektronischen Geschäftsverkehr relevant sein.

3.3.4.2 Gewerbliche Abnehmer

Im Bereich der gewerblichen Abnehmer entsteht im Rahmen der Vertragsgestaltung eine gewisse Lockerung dadurch, dass die besonderen Konsumentenschutzvorschriften nicht zu beachten sind. Gleichwohl werden die rechtlichen Beschränkungen im Bereich der Geltungskontrolle – wenn auch im gelockerten Maß – zu beachten sein. Ebenso sind die Bestimmungen über den elektronischen Geschäftsverkehr zu berücksichtigen.

4. Telematikanwendungen in den einzelnen Verkehrsmodi

In diesem Kapitel wird auf die ausgewählten Themenschwerpunkte innerhalb der einzelnen Verkehrsträger eingegangen. Die Verkehrsdatenerfassung ist neben den einzelnen Verkehrsmodi auch hinsichtlich ihrer Quellen zu unterscheiden.

- Manuelle Datenerfassung
    - Verkehrszählungen
- Technologiebasierte Datenerfassung
    - Induktionsschleifen
    - Radar-, Infrarot- oder Lasertechnik
    - Floating Car Data
    - Mobile Funksysteme (RFID, Bluetooth)
    - Satellitenortung (GPS)
    - Dedicated Short Range Communication (DSRC)

In den folgenden Abschnitten wird besonders das Zusammenspiel zwischen Verkehrsinformationen und kommerziellen Applikationen erläutert. Hier besteht einerseits großes Potential für neue Anwendungen und andererseits sind hier viele Konfliktmöglichkeiten besonders im Bezug auf die Datenweitergabe gegeben.

4.1 Straßenverkehr

Die Einsatzbereiche der Telematik im Straßenverkehr lassen sich wie folgt einteilen.

Tabelle 4-1: Einsatzbereiche der Telematik im Straßenverkehr (Quelle: ITS Handbuch, erweitert durch das Projektteam)

Verkehrssteuerung	Unterstützungssysteme	Informationssysteme
Verkehrs Management Systeme	Elektronische Zahlungssysteme	Fahrgastinformations-systeme
ÖV-Systeme	Advanced Driving Assistance Systems (ADAS)	Verkehrszustands-erfassung
Security und Blaulicht		

Im Straßenverkehr sind speziell Verkehrsinformationssysteme interessant, wenn es um die Verbreitung und Benutzung von Verkehrsinformation durch Dritte geht. In diesem Kapitel wird auf die für Österreich entwickelten Systeme in diesem Bereich Bezug genommen.

4.1.1 Verkehrszustandserfassung

Die rechtlichen Grundlagen der Verkehrszustandserfassung sollen anhand der Projekte FLEET und GO-SMART erläutert werden.

FLEET

Im Projekt FLEET („Fleet Logistics Service Enhancement with Egnos & Galileo Satellite Technology“) wurde ein Reisezeit-Informationsdienst für den Raum Wien auf Basis von Floating Car Data („FCD“) entwickelt und demonstriert.

Die FCD werden periodisch von den On-Board Units in Fahrzeugen einer Taxiflotte abgefragt und enthalten unter anderem die aktuelle Position laut GPS-Modul sowie einen Zeitstempel. Jeder Fahrtauftrag besteht aus einer Reihe dieser Positionen.

Aus diesen Informationen werden im FLEET-System (siehe Abbildung 4-1: Systemübersicht FLEET) durch Map Matching (Verorten des Fahrzeugs auf einem digitalen Straßennetz) und Routing (Ermitteln der zurückgelegten Strecke auf besagtem Straßennetz) Einzelreisezeiten bzw. Geschwindigkeiten berechnet. Diese werden pro Zeiteinheit und Straßenabschnitt aggregiert und so eine Aussage über den Verkehrszustand ermittelt. Des Weiteren werden Kurzfristprognosen über die Verkehrszustandsentwicklung unter Verwendung stochastischer Modelle für die Zeitreihenanalyse generiert.

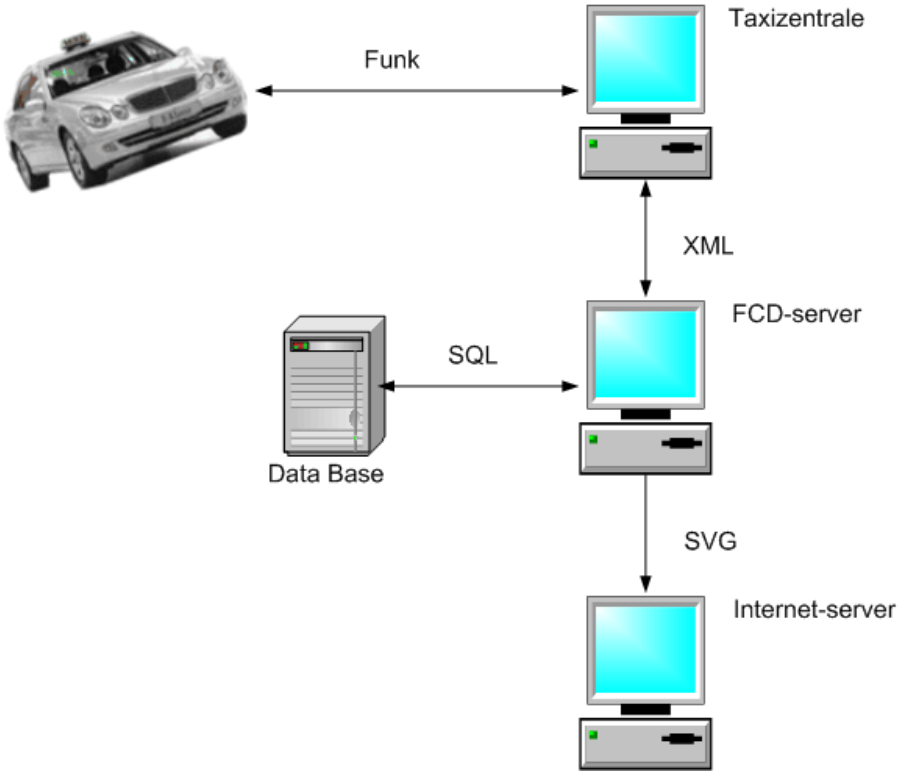


Abbildung 4-1: Systemübersicht FLEET

Aus Datenschutzgründen werden von der Taxizentrale an das System „FLEET“ keinerlei personenbezogenen Daten (Kunde, Lenker, Fahrzeug) weitergegeben. Jeder Fahrtauftrag erhält lediglich eine fortlaufende Nummer, durch die die einzelnen

Fahrzeugpositionen jeweils zu Fahrten zusammengefasst verarbeitet werden können. [FLEET_Endbericht.doc]

4.1.1.1 Rechtliche Einstufung

Auf der Grundlage der vorstehenden Beschreibung stellen sich vor dem Hintergrund der allgemeinen Darstellung in Kapitel 2 vor allem folgende rechtlichen Fragestellungen:

4.1.1.1.1 Ausgangslage

Für die rechtliche Bewertung sind zunächst drei Beteiligte zu identifizieren:

- Betreiber des FLEET-System (im Folgenden „Betreiber“)
- Taxizentrale als Vorleister (im Folgenden „Vorleister“)
- Nachfrage des Informationsdienstes (im Folgenden „Nutzer“)

4.1.1.1.2 Datenschutz

Der Anwendungsbereich des Datenschutzrechts ist für den Betreiber in Bezug auf die Positions- und Zeitangaben nicht eröffnet. Denn ihm ist es nicht möglich, die Positions- und Zeitangaben einer natürlichen Person zuzuordnen. Auch im Rahmen der Verwendung der Daten werden diese keiner natürlichen Person zugeordnet. Datenschutzrechtliche Vorgaben müssen bei der Erhebung und Verwendung der Positions- und Zeitangaben nicht berücksichtigt werden (es liegen keine personenbezogenen Daten vor).

Es wird dabei unterstellt, dass der Vorleister die Daten, insbesondere Positions- und Zeitangaben, datenschutzkonform erhoben hat. Der Betreiber sollte sich dies vertraglich zusichern lassen (Überschneidung zwischen Datenschutzrecht und vertragsrechtlichen Aspekten).

Der Betreiber hat das Datenschutzrecht zu beachten, soweit er personenbezogene Daten über den Nutzer im Rahmen des Vertriebs seiner Zustands- und Prognoseaussagen erlangt. Soweit es sich hierbei nur um Informationen handelt, welche zum Abschluss und zur Abwicklung des Vertrags zwischen Betreiber und Nutzer (im Folgenden: „Nutzungsvertrag“) erforderlich sind, ist von deren Zulässigkeit kraft Gesetzes (siehe etwa §‟7 DSG 2000; § 28 BDSG) auszugehen. Die allgemeinen datenschutzrechtlichen Informationspflichten sind zu beachten.

4.1.1.1.3 Immaterialgüterrecht

Ein immaterialgüterrechtlicher **Schutz der Bereitstellung der Rohdaten** durch den Vorleister ist zu verneinen. Die bloße Bereitstellung von Rohdaten beinhaltet insbesondere keine geistig-schöpferische Leistung (siehe Kapitel 2.2). Der dennoch in Betracht kommende Schutz als Datenbank UrhG setzt voraus

In Österreich:

„Datenbanken im Sinn dieses Gesetzes sind Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind. Ein Computerprogramm, das für die Herstellung oder den Betrieb einer elektronisch zugänglichen Datenbank verwendet wird, ist nicht Bestandteil der Datenbank. Datenbanken werden als Sammelwerke (§ 6) urheberrechtlich geschützt, wenn sie infolge der Auswahl oder Anordnung des Stoffes eine eigentümliche geistige Schöpfung sind (Datenbankwerke).

In Deutschland:

„*Datenbank im Sinne dieses Gesetzes ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Eine in ihrem Inhalt nach Art oder Umfang wesentlich geänderte Datenbank gilt als neue Datenbank, sofern die Änderung eine nach Art oder Umfang wesentliche Investition erfordert.*“

Die bloße Bereitstellung von Rohdaten stellt nach österreichischem und deutschem Recht keine Datenbank im vorgenannten Sinn dar.

Die nach ihrer Aufbereitung zusammengestellten Daten des Betreibers stellen eine solche Datenbank dar und sind rechtlich geschützt. Der Betreiber kann seinen Vertrieb der von ihm geschaffenen Datenbank urheberrechtlich abgesichert gestalten. Zu berücksichtigen ist allerdings, dass die Datenbank in ihre Gesamtheit und nicht eine Einzelinformation, die Bestandteil der Datenbank ist, geschützt ist.

Der Datenbankhersteller hat das ausschließliche Recht, die Datenbank insgesamt oder einen nach Art oder Umfang wesentlichen Teil der Datenbank zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Der Vervielfältigung, Verbreitung oder öffentlichen Wiedergabe eines nach Art oder Umfang wesentlichen Teils der Datenbank steht die wiederholte und systematische Vervielfältigung, Verbreitung oder öffentliche Wiedergabe von nach Art und Umfang unwesentlichen Teilen der Datenbank gleich, sofern diese Handlungen einer normalen Auswertung der Datenbank zuwiderlaufen oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen.

Datenbankhersteller im vorgenannten Sinn ist derjenige, der die Investition im Sinne der Datenbankdefinition vorgenommen hat. Das ist der Betreiber, nicht hingegen seine Mitarbeiter.

Im Rahmen des Vertriebs wird der Betreiber den Nutzern einfache Nutzungsrechte einräumen. Gegebenenfalls kann er diese auch zeitlich begrenzt erteilen.

Daneben kann auch die Software, welche zur Aufbereitung der Daten verwendet wird, als Computerprogramme urheberrechtlich geschützt sein. Da vorliegend die Software nicht vertrieben werden soll, muss dieser Aspekt nicht weiter untersucht werden.

4.1.1.1.4 Vertragsrechtliche Aspekte

Aus Geheimhaltungsgründen liegen die Verträge zwischen Vorleister und Betreiber nicht vor. Darüber hinaus soll im Rahmen dieser Studie auch keine individuelle Vertragsprüfung stattfinden. Eine Prüfung der tatsächlich geschlossenen Verträge erfolgt daher nicht. Es werden grundsätzliche Aspekte der Vertragsgestaltung angesprochen.

Der Betreiber wird im Verhältnis zum Vorleister vor allem drei Interessen haben:

- Bereitstellung der Daten in dem vom Betreiber vorgegeben Format;
- Permanente Verfügbarkeit der Informationen;
- Geheimhaltungspflicht des Vorleisters in Bezug auf Erkenntnisse über die Aufbereitung der Daten durch den Betreiber.

Der Vorleister wird in demselben Verhältnis vor allem das Interesse einer Begrenzung seiner Haftung entsprechend seiner „Leistungsfähigkeit“ mit Blick auf denkbare Folgeschäden beim Nutzer haben.

Die ersten der beiden vorgenannten Interessen werden durch die tatsächliche Leistungsbeschreibung so konkret zu regeln sein, dass beiden Vertragsparteien die Pflichten eindeutig bewusst sind. Durch eine möglichst konkrete Abstimmung werden auch Leistungsgrenzen des Vorleisters für den Betreiber kalkulierbar. Die Geheimhaltung wird als juristische Vertragsregelung eingreifen.

Geltungskontrollrechtliche Beschränkungen (in Deutschland: AGB-rechtliche Beschränkungen) können dann in Betracht kommen, wenn eine der beiden Vertragsparteien auf durch sie standardmäßig verwendete Klauseln zurückgreift. Denkbar ist das insbesondere für die Haftungsbegrenzung und die Geheimhaltungsvereinbarung.

Im Verhältnis des Betreibers zum Nutzer wird es für die rechtliche Bewertung maßgeblich darauf ankommen, ob der Nutzer Verbraucher ist oder nicht. Der Betreiber wird in dieser Beziehung vor allem drei Interessen haben:

- Klarstellung der Informationsqualität;
- Begrenzung seiner Haftung für Mängel der Informationsqualität;
- Schutz der bereitgestellten Information gegen kommerzielle Weiterverwertung durch den Nutzer ohne Beteiligung des Betreibers;

Die Klarstellung der Informationsqualität erfolgt über eine verständliche Leistungsbeschreibung. Diese Klarstellung ist auch mit Blick auf eine wirksame Haftungsbegrenzung erforderlich, da der Nutzer sich dann auch auf eventuelle Risiken einstellen muss. Die Begrenzung der Haftung bezieht sich insbesondere auf Folgeschäden, welche dem Nutzer durch unzutreffende Informationen entstehen können. Wird die Haftungsbegrenzung insbesondere aufgrund der Mehrzahl der Nutzer nicht individuell mit dem Nutzer ausgehandelt, sind die Gestaltungsmöglichkeiten nach österreichischem Haftungsrecht (in Deutschland: die

recht engen Zulässigkeitsgrenzen des AGB-Rechts) zu beachten. Ein Verstoß gegen diese führt zur unbeschränkten gesetzlichen Haftung.

Davon ausgehend, dass ein „Massenabsatz“ dieser Information an Nutzer erfolgt und der Betreiber in seiner Leistungsfähigkeit aufgrund der Leistung des Vorleisters begrenzt ist, wird ein Eingehen auf besondere Wünsche des Nutzers in Bezug auf die Qualität und/oder Verfügbarkeit der Information tatsächlich nicht in Betracht kommen. Die Vertragsregelungen werden daher primär durch Betreiber vorgegeben.

Soweit die Nutzer Verbraucher sind, müssen darüber hinaus auch die besonderen Konsumentenschutzbestimmungen berücksichtigt werden. Vorliegend wird dies vor allem das Fernabsatzrecht sein. Den Betreiber treffen daher umfangreiche Informationspflichten. Darüber hinaus muss er im Rahmen des gesetzlichen Rahmens sicherstellen, dass der Nutzer nicht das nachträgliche Widerrufrecht nach dem Fernabsatzrecht ausüben kann. Das deutsche Fernabsatzrecht sieht Möglichkeiten zum Ausschluss des Widerrufrechts vor, wenn die Leistung kraft Natur der Sache im Fall des Widerrufs durch den Verbraucher nicht mehr zurück gegeben werden kann.

GO-SMART

Im Jänner 2004 wurde auf Österreichs höherrangigem Straßennetz ein Road Pricing System für Fahrzeuge über 3,5 t höchstzulässiges Gesamtgewicht (hzG) eingeführt und die entsprechende Infrastruktur realisiert. Fahrzeuge erzeugen beim Passieren einer Mautstation einen Datensatz, der unter anderem die Identifikation des Straßenabschnittes (Strecke zwischen zwei Mautstationen), die Identifikation des Fahrzeuges, die Achszahl des Fahrzeuges sowie einen Zeitstempel enthält. Des Weiteren werden Querschnittsdaten erhoben. Aus diesen Daten können in Folge beispielsweise Reisezeiten bzw. Geschwindigkeiten berechnet werden. [Das Mautsystem und seine Mehrwerte.pdf]
Ziel des Projekts GO-Smart (Smart Mobility Analysis of Real-time Toll-Data) war es, aus den Mautdaten qualitativ hochwertige Verkehrsinformationen zu generieren. Im Rahmen des Projekts erfolgte die prototypische Umsetzung von Modulen zur Reisezeitberechnung sowie der Filterung und Aggregierung von Reisezeiten und Umrechnung in Geschwindigkeiten. Auf dieser Datengrundlage erfolgt dann eine Schätzung und Prognose des Verkehrszustandes basierend auf klassischen Methoden der Zeitreihenanalyse, wie Autoregressive Integrated Moving Average (ARIMA), und der Künstlichen Intelligenz, wie zum Beispiel Self Organising Maps (SOM).

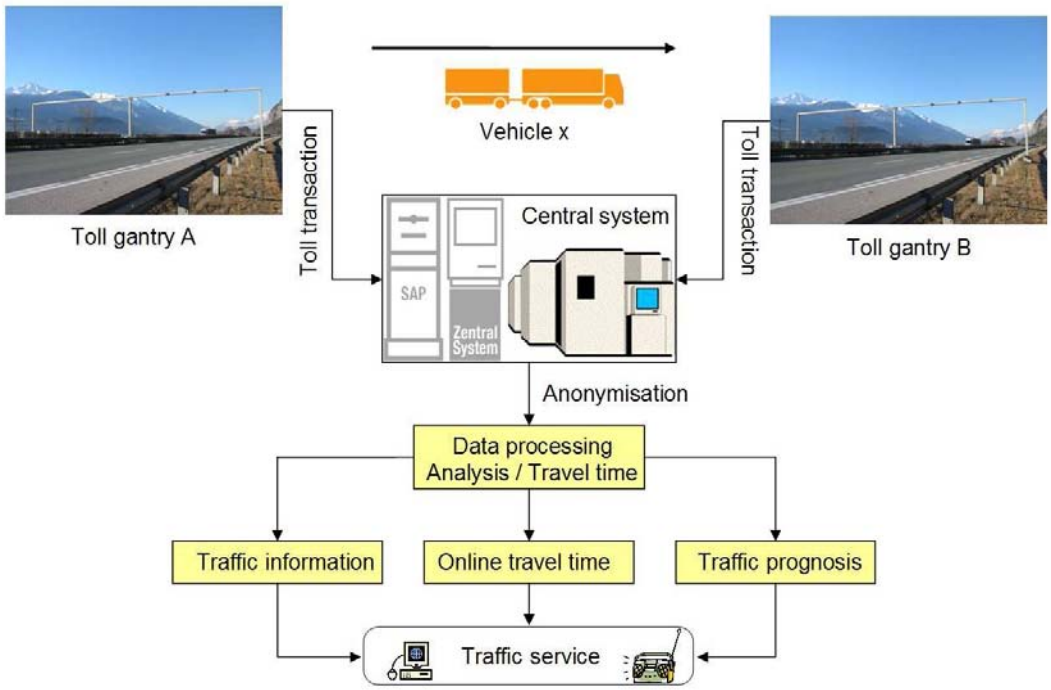


Abbildung 4-2: Systemübersicht GO-Smart

Um die Sicherheit der Verkehrsdaten (Datenschutz) zu gewährleisten, werden Daten zwischen den Projektpartnern ausschließlich über gesicherte (verschlüsselte) Übertragungswege übertragen. Indirekt personenbezogene Daten werden schon vor der Übertragung mittels kryptografischer Hash-Funktionen unumkehrbar anonymisiert. Rechtliche Sicherheitsmaßnahmen wie Datenschutzerklärungen wurden aufgesetzt und von den Projektpartnern unterzeichnet.

In Zusammenarbeit mit der Rechtsabteilung der ASFINAG Holding wurden die relevanten Punkte im Vorfeld hinsichtlich der Anonymisierung der verwendeten Daten analysiert. Die Art der Datenverarbeitung und der verwendeten Verschlüsselung (Anonymisierung im Sinne des Datenschutzgesetzes) wurden sichergestellt. Weitergereicht werden die Daten nur in anonymisierter Form, d.h., dass diese niemand (sohin auch nicht ASFINAG) aufgrund der vorgenommenen Verschlüsselung mehr auf eine, in ihrer Identität bestimmte, Person zurückführen kann. Derartige Daten sind daher auch nicht datenschutzrelevant (Dohr/Pollirer/Weiß, DSG2 (2002) § 4 Anm. zu Z 2). Details dazu sind im ASFINAG Aktenvermerk MSG/2006/000324 zu finden.

Im Zuge der Umsetzung des Projektes „GO-SMART“ werden Daten aus dem Zentralsystem des österreichischen LKW-Mautsystems über eine automatische Schnittstelle an eine Applikation weitergereicht, die nicht im Zusammenhang mit der Verarbeitung und Abrechnung von Mauttransaktionen steht, sondern diese übermittelten Daten mit statistischen Verfahren auswertet. Zu diesem Zweck muss

ein einzelnes Fahrzeug identifizierbar bleiben, damit die Fahrzeiten zwischen den einzelnen Mautportalen berechnet werden können.

Es werden im Projekt keine Fahrtrouten einzelner Fahrzeuge rekonstruiert, bzw. einzelne Fahrzeuge über mehrere Mautportale „verfolgt“. Ebenso werden keine Bewegungsmuster individueller Fahrzeuge berechnet oder dargestellt. [Endbericht_GO-SMART_V1-0 FINAL.pdf]

4.1.1.2 Rechtliche Einstufung

Auf der Grundlage der vorstehenden Beschreibung stellen sich vor dem Hintergrund der allgemeinen Darstellung in Kapitel 2 vor allem folgende rechtlichen Fragestellungen:

4.1.1.2.1 Ausgangslage

Aufgrund der für die rechtlichen Fragen sehr ähnlichen Typologie zu FLEET, ist zunächst auf die Ergebnisse in der rechtlichen Einstufung zu FLEET zu verweisen.

Für die rechtliche Bewertung sind zunächst drei Beteiligte zu identifizieren:

- Betreiber des GO-SMART-System (im Folgenden „Betreiber“), der gleichzeitig auch die Daten erzeugt;
- Nachfrage des Informationsdienstes (im Folgenden „Nutzer“)

4.1.1.2.2 Datenschutz

Der Anwendungsbereich des Datenschutzrechts ist für den Betreiber in Bezug auf die Positions- und Zeitangaben auch in diesem Projekt nicht eröffnet. Es wurde laut dem obenstehenden Sachverhalt alles getan, um die Personenbezogenheit von Daten zu vermeiden).

4.1.1.2.3 Immaterialgüterrecht

Auch im Projekt GO-Smart stellen die, nach ihrer Aufbereitung zusammengestellten Daten des Betreibers eine Datenbank dar und sind rechtlich geschützt. Der Betreiber kann seinen Vertrieb der von ihm geschaffenen Datenbank urheberrechtlich abgesichert gestalten. Im Detail wird auf die Ausführungen zu FLEET verwiesen.

4.1.1.2.4 Vertragsrechtliche Aspekte

Da der Betreiber die Daten nicht von einem Vorleister bezieht, ist dieses Verhältnis nicht zu untersuchen. Relevant ist allenfalls auf einer vorgelagerten Stufe das rechtliche Verhältnis des Betreibers zu seinen Systemlieferanten, auf das allerdings im Rahmen dieser Studie nicht weiter eingegangen wird. Es ist davon auszugehen, dass der Betreiber beim Abschluss der Verträge mit Systemlieferanten darauf geachtet hat, dass die gelieferten Systeme die erforderliche Datenerfassung auch gewährleisten (Kauf- und Werkvertragsrecht)

Im Verhältnis zum Nutzer wird der Betreiber wie schon bei FLEET vor allem drei Interessen haben:

- Klarstellung der Informationsqualität;
- Begrenzung seiner Haftung für Mängel der Informationsqualität;
- Schutz der bereitgestellten Information gegen kommerzielle Weiterverwertung durch den Nutzer ohne Beteiligung des Betreibers;

Im Übrigen wird auf die ausführliche Darstellung zu FLEET verweisen.

4.1.2 Enforcement

Videoerfassung von Daten und Videoüberwachungsanwendungen sind stark datenschutzkritische Themenbereiche der Verkehrstelematik. Im Folgenden sollen zwei Anwendungen im Bereich der Videosysteme näher erläutert werden und die rechtlich betroffenen Rechtsbereiche im Anschluss daran analysiert werden.

Rotlichtüberwachung an Eisenbahnkreuzungen

Das System besteht aus zwei Bestandteilen die im Folgenden kurz beschrieben werden.

- **Videokamera**: Die Videokamera erfasst alle sich nähernden Fahrzeuge mit retroreflektierenden Kennzeichen an der Fahrzeugfront (LPR), deren Bewegungsrichtung, Zeitpunkt der Erfassung und Haltevorgänge. Die Videokamera ist zusätzlich mit einer Lichtquelle ausgestattet (je nach Bedarf intern oder extern).
- **Rotlichtdetektor**: Der Rotlichtdetektor erfasst, ob die Lichtsignalanlage rot geschaltet ist.
- **Datenfernübertragungseinrichtung - DFÜ**: Die DFÜ ist verantwortlich für die Datenübertragung zwischen der Videokamera und der Zentrale.

Das System steht in 2 Varianten zur Verfügung:

- **System mit autarker Energieversorgung:** Dieses System eignet sich speziell für technisch nicht gesicherte Eisenbahnkreuzungen, da bei diesen keine externe Energieversorgung vorhanden ist. Die Energieversorgung des Systems erfolgt durch Akkus und Solarzellen.
- **System mit externer Energieversorgung:** Dieses System eignet sich besonders für technisch gesicherte Eisenbahnkreuzungen, da bei diesen der Zugriff zur Energieversorgung der Sicherungsanlage möglich ist.

Die Eisenbahnkreuzung wird von einer Videokamera überwacht (siehe Abbildung 4-3). Die Videokamera erfasst das Kennzeichen und speichert dieses zusammen mit

einem Bild des Fahrzeuges und weiteren Daten wie zum Beispiel Haltevorgang, Zeit der Erfassung und Bewegungsrichtung. Missachtet der Fahrzeuglenker das Haltegebot (Andreaskreuz) oder das Rotlicht und überquert unerlaubt den Bahnübergang, werden die aufgezeichneten Daten über die Datenfernübertragungseinrichtung an die Zentrale geschickt, wo dann das Vergehen unter anderem geahndet werden kann.

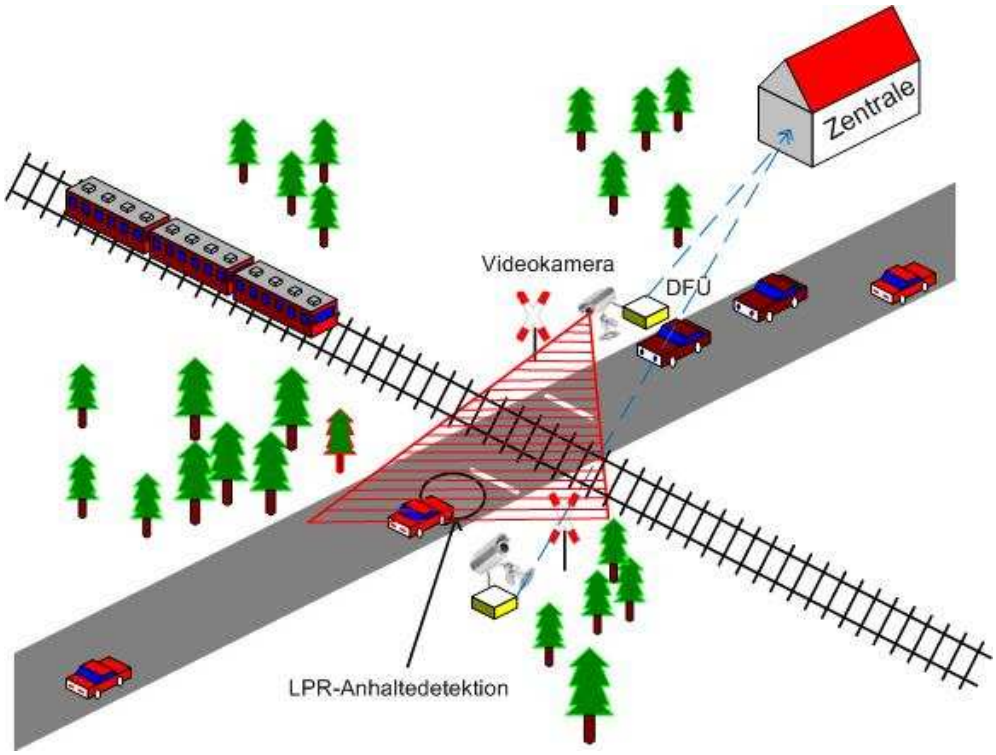


Abbildung 4-3: Systemskizze Red Light Enforcement an Eisenbahnkreuzungen

4.1.2.1 Rechtliche Einstufung

Hier stehen datenschutzrechtliche Fragen im Vordergrund. War bislang die Videoüberwachung an Eisenbahnkreuzungen nicht zulässig, so hat die Novelle zum Eisenbahngesetz im Jahr 2010 die rechtlichen Rahmenbedingungen dafür geschaffen und ermöglich längst überfällige Verbesserungen für die Sicherheit auf Eisenbahnkreuzungen. Analog zur StVO wird die rechtliche Möglichkeit für den Einsatz von Überwachungskameras und Aufzeichnungen geschaffen, für die Übertretung des Anhaltegebots durch Rotlicht und die Überschreitung von Geschwindigkeitslimits. Die Gesetzesänderung erfolgte vor dem Hintergrund von 167 Unfällen auf Eisenbahnkreuzungen im Jahr 2009 mit 14 Toten.

Der Abänderungsantrag war mit den wesentlichen Beteiligten (Gemeindebund, Wirtschaftskammer; Eisenbahnunternehmen; BMI und Bundeskanzleramt) abgestimmt. Die Änderung war in dieser Weise notwendig, weil analog zur StVO bei der Überwachung von Eisenbahnkreuzungen strenge datenschutzrechtliche Bestimmungen gelten.

Unter dem Titel „Bildverarbeitende technische Einrichtungen“ enthält das Eisenbahngesetz in der geltenden Fassung die Ermächtigung zum Einsatz bildverarbeitender, technischer Einrichtungen. Der Text lautet wie folgt:

Für Zwecke der automationsunterstützten Feststellung einer entgegen einer Verordnung nach § 49 Abs. 3 im Bereich von schienengleichen Eisenbahnübergängen durch Verkehrsteilnehmer begangenen
1. Missachtung eines von einer Sicherungsanlage abgegebenen Rotlichtzeichens, oder
2. Überschreitung einer ziffernmäßig festgesetzten zulässigen Höchstgeschwindigkeit

dürfen Bezirksverwaltungsbehörden, im örtlichen Wirkungsbereich einer Bundespolizeidirektion diese, zwecks verwaltungsstrafrechtlicher Ahndung solcher Zuwiderhandlungen gegen eine Verordnung nach § 49 Abs. 3 bildverarbeitende technische Einrichtungen, im Falle der Z 2 solche, mit denen die Fahrgeschwindigkeit eines Fahrzeuges an einem Punkt gemessen werden kann (punktuelle Geschwindigkeitsmessung), verwenden. Diese technischen Einrichtungen umfassen jeweils alle Anlagenteile, die diesem Zweck dienen.

Die Ermittlung von Daten, die zur Identifizierung von Fahrzeugen oder Verkehrsteilnehmern geeignet sind, mittels Einrichtungen gemäß Abs. 1 ist jeweils auf den Fall einer festgestellten Missachtung eines Rotlichtzeichens oder jeweils auf den Fall einer festgestellten Überschreitung einer ziffernmäßig festgesetzten zulässigen Höchstgeschwindigkeit zu beschränken. Soweit die bildgebende Erfassung von Personen, die keine Verwaltungsübertretung begangen haben, technisch nicht ausgeschlossen werden kann, sind die Daten dieser Personen ohne unnötigen Verzug in nicht rückführbarer Weise unkenntlich zu machen.

Gemäß Abs. 1 ermittelte Daten dürfen ausschließlich für die Identifizierung des Fahrzeuges oder des Verkehrsteilnehmers verwendet werden, und zwar ausschließlich für Zwecke eines Verwaltungsstrafverfahrens wegen Missachtung eines Rotlichtzeichens oder einer Überschreitung einer ziffernmäßig festgesetzten zulässigen Höchstgeschwindigkeit.

Ob im Bereich eines schienengleichen Eisenbahnüberganges für die automationsunterstützte Feststellung einer der im Abs. 1 genannten Verwaltungsübertretungen von einem zum Bau und zum Betrieb einer Eisenbahn berechtigten Eisenbahnunternehmen eine bildverarbeitende technische Einrichtung einzurichten ist, hat die Behörde im Einzelfall nach Maßgabe der örtlichen Verhältnisse und Verkehrserfordernisse zu entscheiden. Die eingerichteten bildverarbeitenden technischen Einrichtungen sind den im Abs. 1 angeführten Bezirksverwaltungsbehörden und Bundespolizeidirektionen zur Verwendung zugänglich zu machen. Die Träger der Straßenbaulast sind zur kostenlosen Duldung der Anbringung von bildverarbeitenden technischen Einrichtungen oder

Anlagenteilen solcher bildverarbeitender technischer Einrichtungen auf Straßengrund verpflichtet.

Generell werden die allgemeinen datenschutzrechtlichen Bestimmungen zur Videoüberwachung (siehe dazu oben Kapitel Exkurs: Videoüberwachung) einzuhalten sein.

Weitere Details werden sich in einer Novelle zur Eisenbahnkreuzungsverordnung finden, die derzeit in Begutachtung befindlich ist (vgl. http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=538993&DstID=0&titel=Entwurf,einer,Eisenbahnkreuzungsverordnung). Wesentliche Themen der Diskussion sind insbesondere die Kosten und Kostentragung für zusätzliche Sicherungsmaßnahmen.

Schutzwegüberwachung

Ziel des Projektes „Schutzwegüberwachung“ ist die Erfassung und Auswertung von Szenarien im Bereich von Schutzwegen mit speziellen Videokameras und Videoanalyseverfahren zur Dokumentation möglicher Gefährdungen von Fußgängern durch Kraftfahrzeuge. Das System detektiert durch Bewegungsanalyse von Personen und Kraftfahrzeugen in Echtzeit mögliche Verstöße gegen §9 Abs. 2 StVO[4] und speichert im Anschluss 1) das Kennzeichen des gefährdenden Kraftfahrzeuges und 2) eine Videosequenz, die das Verhalten des Kfz vor bzw. beim Überfahren des Schutzweges dokumentiert.

Das System wird aus 3 Teilkomponenten aufgebaut:

- Videodetektion von Fußgängern im durch § 9 Abs. 2 StVO gesetzlich festgelegten Bereich am und um den Schutzweg. Der intelligente Sensor erfasst Personen im festgelegten Bereich um den Schutzweg und kombiniert diese Information mit dem Sensor für Fahrzeugkennzeichen, um gefährliche Situationen zu erkennen.

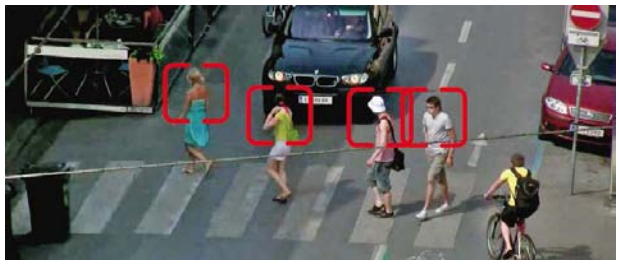


Abbildung 4-4: Pedestrian Detection (Quelle: SLR engineering OG)

4 „*Der Lenker eines Fahrzeuges, das kein Schienenfahrzeug ist, hat einem Fußgänger oder Rollschuhfahrer, der sich auf einem Schutzweg befindet oder diesen erkennbar benützen will, das unbehinderte und ungefährdete Überqueren der Fahrbahn zu ermöglichen. Zu diesem Zweck darf sich der Lenker eines solchen Fahrzeuges einem Schutzweg nur mit einer solchen Geschwindigkeit nähern, dass er das Fahrzeug vor dem Schutzweg anhalten kann, und er hat, falls erforderlich, vor dem Schutzweg anzuhalten. In gleicher Weise hat sich der Lenker eines Fahrzeuges, das kein Schienenfahrzeug ist, vor einer Radfahrerüberfahrt zu verhalten, um einem Radfahrer oder Rollschuhfahrer, der sich auf einer solchen Radfahrerüberfahrt befindet oder diese erkennbar benützen will, das ungefährdete Überqueren der Fahrbahn zu ermöglichen.*“

- Videobasiertes System zur Erfassung und Verfolgung von Fahrzeugkennzeichen passierender Kraftfahrzeuge. Die mit jedem Messzyklus segmentierten Symbole des Zulassungskennzeichens werden in zeitabhängiger Farbcodierung dargestellt, anhand eines Zeitdiagrammes in der Legende können die einzelnen Kennzeichenpositionen eindeutig zeitlich zugeordnet werden.

Die Integration der Teilkomponenten (Stromversorgung, interne Kommunikation, etc.) zur Zusammenführung und Auswertung der Datenströme sowie zur Kommunikation zu einer festzulegenden Auswertungszentrale erfolgt im Sensor für Personendetektion in einem Industrie PC. Dieser speichert und archiviert die Videoströme, und leitet sie an die Auswertungszentrale weiter. Im Testsystem wird vorerst die Archivierung der Daten im Personen-Sensor und ein anschließender Download über das lokale Netz realisiert.

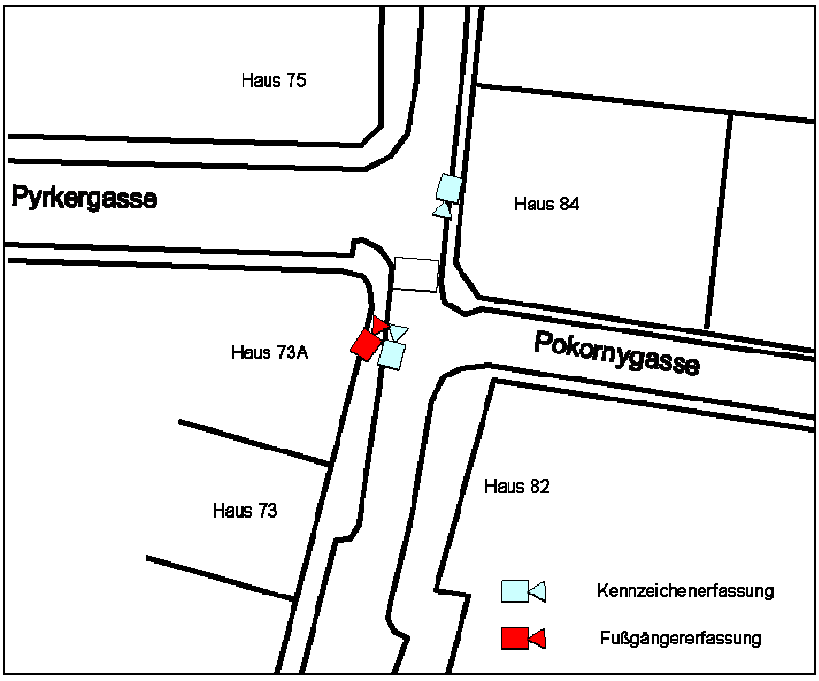


Abbildung 4-5: Standorte Kamerasysteme Schutzwegüberwachung

4.1.2.2 Rechtliche Einstufung

Zwei Rechtsbereiche sind in diesem Projekt betroffen:

- **STVO** §98f Regelung der Überwachung und Verkehrsbeobachtung und §9 Absatz 2 Vormerkdelikt: Die derzeitige Rechtslage schließt eine Überwachung der Schutzwege aus. Eine Änderung der STVO wäre dazu notwendig.
- **Datenschutzgesetz** §46/3 Wissenschaftliche Forschung

Anders als für die Überwachung von Eisenbahnkreuzungen liegt für die Überwachung von Schutzwegen noch keine datenschutzrechtlich ausreichende Ermächtigung im entsprechenden Materiengesetz vor.

Die Verkehrsbeobachtung am Schutzweg kann heute nur gemäß den oben genannten Bestimmungen erfolgen. Übertretungen sind auf Basis der gegenwärtigen Rechtslage nicht verwaltungsstrafrechtlich verfolgbar.

§ 98 f STVO lautet: Soweit dies 1. für die Regelung sowie die Leichtigkeit, Flüssigkeit und Sicherheit des Verkehrs oder 2. für die Erfüllung der den Behörden und Straßenerhaltern gesetzlich obliegenden Aufgaben erforderlich ist, dürfen die Behörden und Straßenerhalter zur Beobachtung des Verkehrsgeschehens technische Einrichtungen zur Bildübertragung einsetzen. Eine bildgebende Erfassung, die eine Identifizierung von Personen oder Fahrzeugen ermöglicht, ist jedoch nur zulässig, soweit dies im Einzelfall zwingend erforderlich ist, um die Aufgaben nach Abs. 1 zu erfüllen. Eine Speicherung von gemäß Abs. 1 gewonnenen Daten ist nicht zulässig. Für Zwecke der Information der Öffentlichkeit im Wege von Medien dürfen im Bedarfsfall auf Anfrage manuell einzelne Bildquellen ausgewählt und daraus kurze Bildfolgen gespeichert und an Medien übermittelt werden, soweit eine Identifizierung von Personen oder Fahrzeugen nicht möglich ist.

Auch das allgemeine Datenschutzrecht stellt hier keine weiterreichenden Mechanismen zur Verfügung insofern eine Datenverwendung allenfalls und unter bestimmten Einschränkungen für wissenschaftliche Forschung und die Statistik zulässig ist.

Ein konkreter Vorschlag aus dieser Studie ist daher darauf gerichtet, eine entsprechende Änderung in der STVO herbeizuführen, vergleichbar der jüngsten Änderung im Eisenbahngesetz (vgl. dort § 50).

4.2 Schienenverkehr

In Tabelle 4-2 sind die Einsatzbereiche der Telematik im Schienenverkehr ersichtlich.

Tabelle 4-2: Einsatzbereich der Telematik im Schienenverkehr (Quelle: Lehrunterlagen DI Alexander Chloupek)

Betriebssteuerung & Sicherung	Ressourcen- & Leistungsdisposition	Kundeninformation & -service
Automatisch Fahr- & Bremssteuerung	Zuglauf- & Fahrzeugverfolgung	Kommunikation im Zug
Trassenbildung	Disposition von Ressourcen	Fahrplan- & Preisinformationen
Eisenbahnkreuzungs-sicherung	Vorrangentscheidungen	Abweichungs-management
Zugvollständigkeits-kontrolle	Vorhersagen, Prognosen	Tracking & Tracing Zustandsinformationen

Elektronischer Fahrplan	Gegensteuermaßnahmen	Erfassen von Kundenwünschen
Zugbildung & Zugtrennung	Konfliktmanagement	Alternativangebot bei Unregelmäßigkeiten
Beweglicher Bremswegabstand	Übersetzung von Kundenwünschen in Dispositionsentscheidungen	Elektronischer Frachtbrief
Zugfolgesicherung Abstandshaltung	Kurzfristiges Einlegen zusätzlicher Züge	Internetticketkauf & -reservierung
Kommunikation	Datenaustausch	Ergänzende Dienstleistungen Multimedia, Hotels, Lagerung
Ortung, Sicherheit	Anschlusssicherheit Intermodale Logistikketten	Mobiles Ticket

Der Schwerpunkt wurde in diesem Kapitel auf die Themenbereiche Infrastrukturmessstellen (am Beispiel RFID) und Lokalisierungsservices (am Beispiel GPS) gelegt, da hier die Weitergabe von Daten ein besonders wichtiges Thema ist.

4.2.1 Infrastrukturmessstellen

Als Beispiel für Infrastrukturmessstellen sollen unterschiedliche RFID Anwendungsgebiete erläutert werden.

Mögliche Einsatzgebiete von **RFID** bei der Bahn sind:

- Fahrzeug- und Frachtverfolgung
- Instandhaltungsoptimierung, Wartung
- Inventarisierung
- Mobile Ticketing

Probleme von RFID (allgemein): RFID Chips können ohne großen finanziellen Aufwand mitgelesen werden, dies ist an und für sich kein Problem, solange die Daten nicht direkt einer Person zugeordnet werden können. Die Fahrzeugnummer, die zum Beispiel mit der RFID Technologie gespeichert und gelesen werden kann, ist auch von den Fahrzeugen selbst ablesbar, weshalb es hier zu keiner Verletzung von Datenschutzrecht kommt.

Statement aus der Studie „RFID Einsatz an Infrastrukturmessstellen“ zum Thema Datenschutz: „Im Bahnbereich kommt die RFID Technologie nicht auf Waren-Ebene, sondern auf Asset-Ebene zum Einsatz, das bedeutet, dass nicht die Ware von

Bedeutung ist, sondern der Waggon selbst. Da die Transpondertechnologie im Bahnbereich nur zur Asset-Identifikation eingesetzt wird und die Daten öffentlich lesbar sind, ist das Datenschutzgesetz in diesem Fall nicht relevant. Das bedeutet, dass die Daten die auf dem Transponder gespeichert sind, mit Hilfe eines Lesegerätes von jeder Person ausgelesen werden können. Dabei handelt es sich aber nur um Wagendaten, wie zum Beispiel die Wagennummer, die Wagenlänge, etc. die auf dem Transponder, anstatt der Aufschrift am Wagen abgespeichert sind. Somit können auf Transponder die mit freiem Auge lesbaren Daten, ohne rechtliches Bedenken gespeichert werden."

Rechtliche Problembereiche zum RFID Einsatz im Bahnbereich ergeben sich hinsichtlich:

- der Verfolgung der Transporte durch Dritte / streckenseitig,
    - Leitstand – RFID-Daten / E-Frachtbrief / etc., Daten können direkt am Leitstand einem Kunden zugeordnet werden
    - Leitstand – Weitergabe der Daten an Dritte
- Mobiles Ticketing:
    - Bezahlung mit RFID-Karte → Daten (Wege) können direkt einer Person zugeordnet werden → Missbrauch durch Dritte möglich
    - Überwachung und Feststellen von Bewegungsmustern
    - Datenverarbeitung bei der Rechnungsstelle → Keine Weitergabe der Daten an Dritte

4.2.1.1 Rechtliche Einstufung

Die Verwendung von RFID-Daten darf gemäß den §§ 6 bis 9 DSG 2000 nur nach Treu und Glauben und auf rechtmäßige Weise erfolgen und die Datenverwendung muss sich an den Zweckbindungsgrundsatz sowie an den Wesentlichkeitsgrundsatz halten. Sowohl bei der Verarbeitung von RFID-Daten als auch bei der Übermittlung dürfen die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. Mit Zustimmung des Betroffenen, wenn lebenswichtige Interessen des Betroffenen berührt sind, bei gesetzlichen Ermächtigung oder Verpflichtung sowie bei der Verarbeitung von indirekten personenbezogenen Daten ist die Datenverwendung von RFID Anwendung ohne Zustimmung zulässig.

Daraus ergibt sich, dass im privaten Bereich die Datenverwendung zur Erfüllung einer vertraglichen Pflicht zwischen Auftraggeber und Betroffenen zulässig ist. Auf die Ausnahmebestimmung des § 46 für die Verwendung zu wissenschaftlichen und statistischen Zwecken haben wir oben bereits hingewiesen.

In den oben beschriebenen Beispielen handelt es sich überwiegend um Wirtschaftsdaten, an deren Geheimhaltung ein schützwürdiges Interesse in der Regel besteht. Datenschutzrechtlich betroffen sind hier neben den Lieferanten wohl auch die Empfänger, insofern sie ein schützwürdiges Geheimhaltungsinteressen haben. In der Regel werden hier in der Kette der Beteiligten konkludente oder

ausdrückliche Zustimmungen vorliegen, die die Datenanwendung rechtmäßig machen. Es ist allerdings darauf hinzuweisen, dass an die Zustimmung strenge Anforderungen gestellt werden.

Bei RFID-Applikationen könnte ferner das Telekommunikationsgesetz TKG 2003 anwendbar sein, wenn die Applikation als öffentlicher Telekommunikationsdienst gewertet wird (vgl. § 3 Ziffer 9 TKG 2003). In der Vielzahl der Fälle wird die RFID-Applikation aber nicht im öffentlichen Bereich stattfinden und deshalb kein öffentlicher Kommunikationsdienst im Sinne des TKG 2003 sein.

Im Bereich des Mobile Ticketing wie oben beschrieben, kann die RFID Applikation ausschließlich mit Zustimmung der betroffenen Person erfolgen. Aber auch mit der Zustimmung ist darauf zu achten, dass die Vorschriften des Datenschutzgesetzes eingehalten werden.

4.2.2 Location Based Services

Tracking und Tracing von Wagen/Containern ist zum Beispiel mit dem CargoObserver, einem Produkt aus dem Forschungs- und Entwicklungsprojekt WCMS/BOX, möglich.

Das CargoObserver System ist ein GPS und GSM unterstütztes drahtloses Sensorsystem für die Zustandsüberwachung und Positionsverfolgung von Containern. Das Basissystem besteht aus einer Master Telematics Unit (MTU), die eine Kommunikationseinheit und Basissensoren zur Verfügung stellt (aus [4W]).

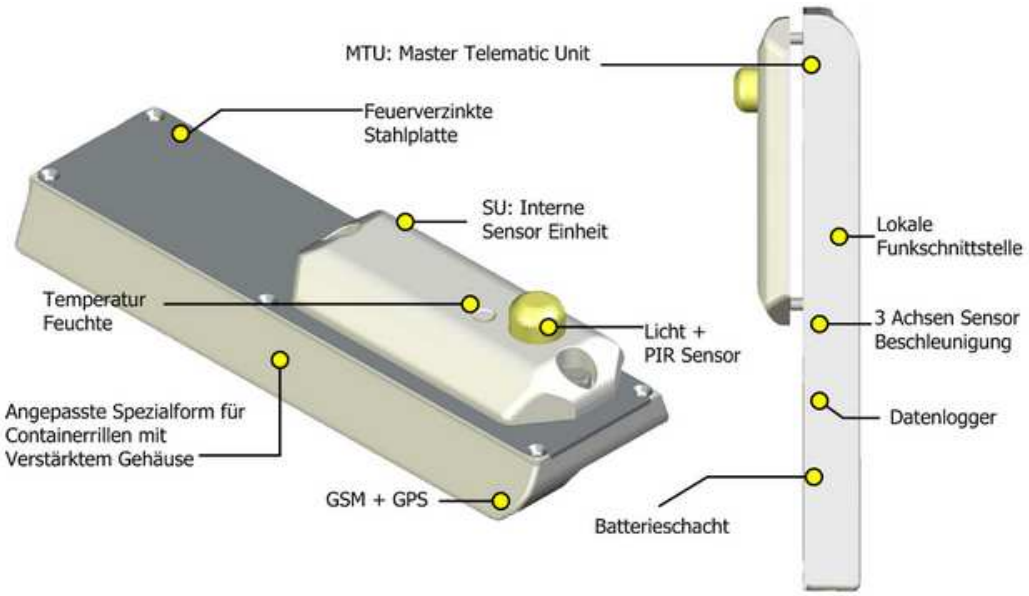


Abbildung 4-6: CargoObserver MTU

Als Erweiterung können eine oder mehrere interne Sensoreinheiten (Sensor Units, „SU“) hinzugefügt werden. Diese übernehmen weitere Funktionen, wie Temperatur-, Feuchte- oder Einbruchsüberwachung und können drahtgebunden oder drahtlos an das System gekoppelt werden. Die Energieversorgung übernehmen Lithium-Batterien. Der Vorteil liegt darin, dass das System weltweit verwendet werden kann, dass die SU individuell nach Kundenwunsch mit Sensoren erweitert werden kann, in

der langen Lebensdauer der Lithium-Batterien und dem günstigen Anschaffungspreis (siehe [4W]).

Abbildung 4-7: Einsatz CargoObserver

Rechtliche Problembereiche zum GPS/RFID Einsatz im Bahnbereich ergeben sich vor allem hinsichtlich:

- der Datenweitergabe: Welche Daten werden an wen weiter gegeben? Sind diese Daten schutzwürdig seitens des Datenschutzgesetzes?
- Erhält genau der Richtige die Daten?
- der genauen Verfolgung der Waren: Erkenntnis „Wer beliefert Wen, Wo und Wann?“ → Datenmissbrauch möglich

4.2.2.1 Rechtliche Einstufung

Die Daten, die Gegenstand dieses Verkehrstelematikprojekts sind, sind weder direkt noch indirekt personenbezogen, sodass das Datenschutzrecht idR nicht betroffen sein wird.

Auch immaterialgüterrechtliche Fragen stellen sich nicht primär, sondern allenfalls auf einer technischen Ebene im Verhältnis zwischen dem Betreiber des Systems und seinen Systemlieferanten.

In Zentrum stehen allerdings vertragsrechtliche Fragen zwischen dem Betreiber des Systems und den Nutzern. Die oben angesprochenen Fragen sind vorweg einer detaillierten vertraglichen Regelung zu unterwerfen. Besonders kritisch erachten wir in diesem Projekt die Frage der Haftung für eine Irrleitung der Güter, eine Beschädigung bzw. eine Übermittlung von Daten an den Nichtberechtigten und allfällige Wettbewerbsverzerrungen daraus. Die Nutzer eines solchen Systems werden sich typischerweise gegen allfällige Risiken absichern wollen und mit dem Systembetreiber entsprechende Pönalen vereinbaren wollen.

4.3 (Binnen)Schifffahrt

Nachfolgende Tabelle stellt die Einsatzbereiche der Telematik in der (Binnen-) Schifffahrt dar.

Tabelle 4-3: Einsatzbereiche der Telematik in der Schifffahrt

Nautische Unterstützung an Bord	Verkehrsmanagement	Fracht und Flottenmanagement
Informationssysteme	Schleusenmanagement	
	Hafenmanagement	

In der Diplomarbeit „Erfolgreiche Einführung von Technologieentwicklungen für Intelligente Verkehrs- und Transportsysteme am Markt“ wird das in Österreich wichtigste Telematiksystem der Schifffahrt, das River Information Services (RIS), beschrieben. Dieses System dient dem Verkehrsmanagement auf Binnengewässern (und insbesondere Wasserstraßen, wie Flüsse). Anfang 2006 wurde in Österreich das nach einem Konzept der via donau – Österreichische Wasserstraßen-Gesellschaft m.b.H. in Zusammenarbeit mit der Obersten Schifffahrtsbehörde System **Donau River Information Services** (DoRIS) in Betrieb genommen. Im Rahmen des EU Projekts COMPRIS erfolgte eine Kooperation mit den Donauländern, um eine umfassende Implementierung von RIS in Europa zu gewährleisten.

Die Hauptfunktion von DoRIS ist die Erfassung und Darstellung der Schiffe auf einer elektronischen Karte (ENC – Electronic Navigational Chart). Dazu werden die wichtigsten nautischen Informationen über das Fahrwasser sowie die Verkehrsregelung angezeigt. Hauptelemente von DoRIS sind die Automatic Identification System-Transponder (AIS). AIS ermöglicht die Bestimmung der aktuellen Position mittels GPS und den Austausch der Positionsinformationen mit anderen ausgerüsteten Schiffen und den landseitigen Einrichtungen durch eine im Transponder eingebaute Datenfunkanlage.

DoRIS verarbeitet neben statischen Daten, die der Schiffsführer eingibt (z.B. Schiffs- und Verbandstyp, maximaler Tiefgang, Zielhafen und geschätzte Ankunftszeit, etc.) auch dynamische Daten, wie Kurs und Geschwindigkeit, die der AIS-Transponder laufend automatisch er- und übermittelt. Zur Darstellung des aktuellen Verkehrsbildes wird der ECDIS-Viewer (Electronic Chart Display and Information System) herangezogen siehe Abbildung 4-8).

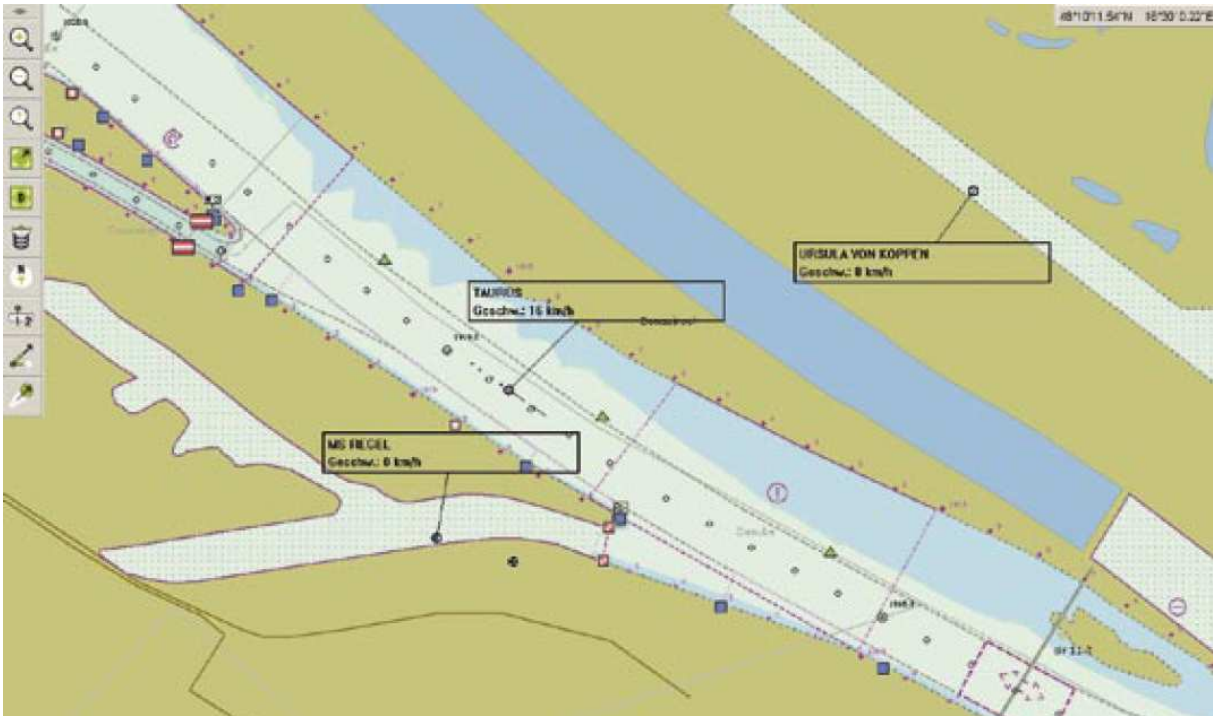


Abbildung 4-8: Taktisches Verkehrsbild DoRIS

Die Basisstationen entlang des Ufers (Abbildung 4-9 zeigt deren Standorte) dienen der Abfrage von DoRIS-Daten an Land, um Schiffsdaten empfangen, weiterleiten und als Basis für weitere Services in der nationalen Leitstelle verarbeiten zu können.

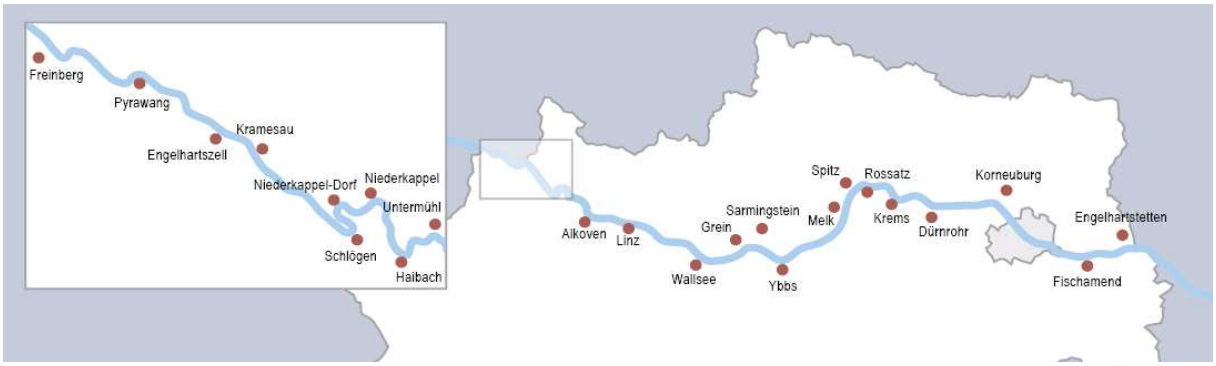


Abbildung 4-9: DoRIS Basisstationen in Österreich

4.3.1.1 Rechtliche Einstufung

Im Dokument „Rechtliche Rahmenbedingungen für den Betrieb von River Information Services“ der ARGE DoRIS werden bereits ausführlich die rechtlichen Rahmenbedingungen für das Donau River Information Services abgehandelt. Darin werden sowohl Völker- und Europarecht, öffentliches Recht (inkl. DSG) und das Zivilrecht im Bezug auf DoRIS untersucht. Aufgrund der Komplexität der Themen in der Studie, kann an dieser Stelle nur auf die über 20-seitige Zusammenfassung verwiesen werden. Abgesehen von den sehr spezifischen völkerrechtlichen Fragestellungen, stehen datenschutzrechtliche und haftungsrechtliche Fragen im Zentrum der Analyse.

4.4 Luftfahrt

Bei den Systemen, die der Flugsicherung (in Österreich der Austro Control) zugehören, gibt es grundsätzlich die Unterscheidung zwischen „Airborne“ und „Ground-based“ Systemen. Diese Technologien bilden in der Luftfahrt die Basis zur Kontrolle, Steuerung und Sicherung des Verkehrs in der Luft.

Firmenintern werden hingegen Transport- & Logistiktools eingesetzt, um die Planung rund um den Air Cargo Transport zu erstellen.

Tabelle 4-4: Einsatzbereiche der Telematik in der Luftfahrt (Quelle: Austro Control, erweitert durch das Projektteam)

Flugsicherung	Transport- & Logistiktools
Kommunikation	
Navigation	
Surveillance (Kontrolle)	
(Data Processing)	

In der Luftfahrt finden sich Telematik-Systeme mit einer Datenweitergabe hauptsächlich im Bereich der Flugsicherung. Weitere Anwendungen im Bereich der Transport- und Logistik unterscheiden sich firmenintern (z.B. nach Schnittstelle, Aufgabe und Tätigkeitsbereich). Bei DHL beispielsweise werden bei den Branchenlösungen der Luftfahrt folgende Bereiche unterschieden:

- Inbound to Manufacturing-Logistik (I2M)
- Fertigungslogistik
- Lagerhaltung & Auftragsabwicklung
- Transportmanagement und Distributionslogistik
- Aftermarket-Logistik in der Luftfahrt
- Optimierte Fertigungslogistik
- Aircraft On Ground
- Umgestaltung der Supply Chain für die Bordverpflegung
- Supply-Chain-Analyse und -Konzeption
- Spezialtransporte für die Luftfahrtindustrie

Datenschutzrechtlich ist danach zu unterscheiden ob überhaupt direkt oder indirekt personenbezogene Daten verarbeitet werden. Nur soweit dies ausnahmsweise überhaupt der Fall ist, stellt sich die Frage der Anwendbarkeit des DSG 2000.

Vertragsrechtlich stellen sich die in Kapitel 2 generell dargestellten Fragestellungen mit in diesem Bereich typischerweise multiplen Vertragsbeziehungen aufgrund der Involvierung mehrerer Beteiligter. Themen der rechtzeitigen Anlieferung und sich daraus ergebende Haftungsfragen stehen im Zentrum.

4.5 Intermodaler Verkehr

ITS Vienna Region ist das Verkehrsmanagementprojekt der Länder Wien, Niederösterreich und Burgenland. Es wurde 2006 als eigenständiges Projekt im VOR gegründet. Seit 2009 ist der neue Routenplaner „AnachB.at“ der ITS Vienna Region im Internet unter http://www.anachb.at/ verfügbar. Das Online-Verkehrsservice erlaubt eine Routenplanung für alle Verkehrsarten in Wien, Niederösterreich und Burgenland.

AnachB.at vereint eine Reihe von unterschiedlichen Informationskanälen und bietet im Vergleich zu herkömmlichen Routenplanern folgende zusätzliche Optionen:

- Radroutenplaner sowie Bike and Ride Routenerstellung
- Park & Ride, sowie Anzeige der Auslastung von Parkhäusern
- Auskunft über die Verkehrslage
- Baustellen- und Verkehrsmeldungen

4.5.1.1 Rechtliche Einstufung

ITS Vienna Region ist keine eigene Körperschaft. Die Daten stammen von unterschiedlichen Parteien:

- Länder (Baustellen, Graphen, etc.),
- Ö3 (über einen Kaufvertrag),
- Floating Car Data von Taxibetreibern (über einen Kaufvertrag),
- der ASFINAG im Rahmen eines Kooperationsvertrags
- und den ÖBB.

Die wesentlichste betroffene Rechtsgrundlage für das Projekt des ITS Vienna Region ist das Informationsweitergabegesetz („IWG“ siehe dazu unten). Der Datenschutz ist im Rahmen des Projekts nicht betroffen, da man auf alternative Lösungswege zurück greifen konnte, um die Verarbeitung personenbezogener Daten zu vermeiden:

- Im Rahmen des Projekts VIONA, das sich mit der Erfassung der Reisezeit anhand von Videobildern beschäftigt, werden Kennzeichen zwar gelesen aber sofort gehasht und solcherart die Personenbezogenheit ausgeschlossen.
- Weiters wurden Videokameras montiert, die jedoch zu unscharf und zu weit entfernt sind bzw. so eingestellt sind, dass sie keine personenbezogenen Daten aufnehmen.

Im Sinne des IWG kommt es zu keiner „Datenweitergabe“. Daten werden lediglich von einer öffentlichen Stelle an eine andere öffentliche Stelle zum öffentlichen Zweck weitergegeben und „verwendet“.

Ziel des IWG und der zugrundeliegenden Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors ist es, die Weiterverwendung von Dokumenten öffentlicher Stellen auf ein Mindestniveau anzugleichen, um die Bedingungen für die Nutzung solcher Informationen gerecht, angemessen und nicht diskriminierend zu gestalten. Diese europäische Angleichung soll das Funktionieren des Binnenmarkts und die Entwicklung der Informationsgesellschaft in der Gemeinschaft fördern. Das IWG enthält insofern insbesondere wettbewerbsrechtliche Regelungen.

Das IWG verpflichtet öffentliche Stellen nicht grundsätzlich, Dokumente weiterzugeben. Wenn diese aber Dokumente weitergeben, dann müssen sie die Regelungen des IWG einhalten. Die erstmalige Entscheidung, ob eine Weiterverwendung genehmigt wird, ist Sache der betreffenden öffentlichen Stelle. Sobald aber eine Weiterverwendung von Dokumenten erstmalig gestattet wurde, sind diese in nicht diskriminierender Weise, innerhalb eines bestimmten zeitlichen Rahmens, gegebenenfalls gegen angemessenes Entgelt und grundsätzlich nicht exklusiv auch an jeden Dritten weiterzugeben. Öffentlichen Stellen ist eine eigene wirtschaftliche Nutzung ihrer Dokumente gestattet. Werden Dokumente von öffentlichen Stellen als Ausgangsmaterial für eigene wirtschaftliche Geschäftstätigkeiten verwendet, die nicht unter ihren öffentlichen Auftrag fallen, gelten für diese Tätigkeiten dieselben Bedingungen wie für andere Nutzer.

Weiters kommt es im Rahmen des Projekts zur Nutzung unterschiedlicher Verträge:

- Nutzungsverträge,
- Kooperationsverträge
- und Kaufverträge.

5. Der Umgang mit personenbezogenen Daten – Aktuelle Themenbereiche

5.1 Verkehrsdatenerfassung mit Mobiltelefonen

Datenerfassung auf Basis von Mobiltelefonen gewinnt u.a. durch die Zunahme der Smartphones immer mehr an Bedeutung. Im Rahmen eines F&E Projekts wird ein Mobilfunk-gestütztes Erhebungssystem für den Aktivitätenplanungsprozess entwickelt.

5.1.1 MASI Active

Inhalt des F&E Projekts MASI_active ist die Verwendung von Mobiltelefonen zur automatischen Ortung von Personen, um valide Daten zum Verkehrsverhalten zu erhalten und so eine Qualitätssteigerung und Kostenreduktion bei den Verkehrserhebungen zu erreichen.

Im Projekt MASI_Active ist die Zustimmung zur Verarbeitung personenbezogener Daten der Respondenten zu erreichen und die vorausgegangene ernsthafte und zweifelsfreie Einwilligung verhindert, dass datenschutzrechtlich schutzwürdige Interessen der Respondenten verletzt werden. In diesem Projekt sind allerdings auch verschiedene telekommunikationsrechtliche Bestimmungen zu beachten (Abschnitt 12 Kommunikationsgeheimnis, Datenschutz).

5.1.1.1 Rechtlicher Sachverhalt 1: Befragung

Befragung per SMS: Es wird keine Werbung versandt, daher ist eine Zustimmung telekommunikationsrechtlich nicht erforderlich. Die Zusendung einer elektronischen Post (auch SMS) ist allerdings auch ohne Werbung zu sein ohne vorherige Einwilligung des Empfängers dann unzulässig, wenn sie an mehr als 50 Empfänger gerichtet ist (§ 107 TKG 2003).

Befragung per Anruf zu Statistikzwecken: Wenn keine Werbung vorliegt, ist keine Zustimmung erforderlich Die erhaltenen Daten können dann aufgrund der Bestimmung des § 46 DSG 2000 („Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die öffentlich zugänglich sind oder er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder für ihn nur indirekt personenbezogen sind“) ohne datenschutzrechtliche Genehmigung verwendet werden, sofern sie nicht personenbezogen oder nur indirekt personenbezogen sind. Dies setzt allerdings voraus, dass tatsächlich wissenschaftliche Zwecke oder statistische Untersuchungen Ziel des Projekts sind.

5.1.1.2 Rechtlicher Sachverhalt 2: Einholung und Auswertung der Verkehrsbewertungsinformationen

„Standort Daten“ sind Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Aufenthaltsort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben (§ 92 TKG 2003).

Standortdaten dürfen abgesehen von Notrufdiensten und Verkehrsdaten nur verarbeitet werden, wenn sie anonymisiert werden oder der User eine jederzeit widerrufbare Einwilligung gegeben hat. (§ 102 TKG 2003).

Selbst im Falle einer Einwilligung zur Verarbeitung von Daten müssen die Benutzer oder Teilnehmer die Möglichkeit haben, diese Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu untersagen. Die Verarbeitung anderer Standortdaten als Verkehrsdaten muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

5.2 Mautsysteme

Zur Thematik „Datenschutz in der Verkehrstelematik“ gibt es einen wesentlichen Themenbereich, der fortlaufend in den Medien erwähnt wird: Die Mautsysteme. Sowohl die Weiterverwertung von Mautdaten als auch die Schaffung einer Grundlage für ein einheitliches Mautsystem sind erstmals Themen, an welchen großes Interesse besteht, bei welchen jedoch die rechtlichen Grundlagen zu evaluieren sind.

5.2.1 Schaffung der Grundlage für ein einheitliches Mautsystem

Anfang Oktober 2009 hat die Europäische Kommission eine Entscheidung erlassen, in der die grundlegenden technischen Spezifikationen und Anforderungen für einen einheitlichen europäischen elektronischen Mautdienst (EETS) festgelegt werden. Der Dienst soll eine einfache Einrichtung von Mautgebühren in der gesamten Europäischen Union ermöglichen, mit einem einzigen Vertrag mit einem Dienstleister und nur einem Bordgerät (OBU). Der Dienst wird auf allen Infrastrukturen in der gesamten Gemeinschaft, wie Autobahnen, Tunneln und Brücken, zur Verfügung stehen, wo Mautgebühren über ein Bordgerät erfasst werden.

Dies stellt jedoch erst den Anfang bei der Schaffung einer Grundlage für ein einheitliches Mautsystem in Europa dar.

5.2.2 Die Weiterverwertung von Mautdaten

Laut der deutschen Onlineplattform „heise-online“ soll in Deutschland ein Pilot-Projekt starten, worin Mautdaten verwendet werden, um den Container-Verkehr im Hafengebiet Hamburg zu optimieren. Folgender Auszug stammt aus dem online Artikel vom 03.08.2009 (siehe [5W]).

5.2.2.1 Lkw-Maut: Mautdaten sollen Führungsdaten werden

Eine Hamburger Initiative will die vom Betreiber Toll Collect gesammelten Daten auswerten und mit ihnen in einem "Truck Guide Hamburg" den Container-Verkehr im Hafengebiet optimieren. Drei Jahre nach der Diskussion um die Nutzung der Mautdaten als Fahndungsdaten bei Schwerverbrechen soll die wirtschaftliche Nutzung vor allem den in Zukunft erwarteten Anstieg der Container-Transporte auffangen.

Die Auswertung der LKW-Positionen im Großraum Hamburg wird nach einer Mitteilung der Logistik-Initiative Hamburg helfen, das hohe Transportaufkommen im Hamburger Hafen besser zu steuern. An der Entwicklung des "Truck Guide Hamburg" sind neben dem Mautbetreiber Toll Collect die Hamburg Port Authority, der Container-Logistik-Konzern Eurogate und der Software-Dienstleister Dakosy beteiligt. Dabei wird eine Lotsen-Lösung angestrebt, die an- und abfahrende Container-Transporte optimal durch das Hafengebiet steuert. Das Datenmaterial für diese telematische Lösung soll die fortlaufende Positionsbestimmung der LKW bilden, die der Mautbetreiber Toll Collect zur Verfügung stellen will. Aus dem Material kann neben der Position des Fahrzeugs die Fahrtrichtung und die Geschwindigkeit ermittelt werden. Das Datenmaterial will Toll Collect ab 2010 für einen auf zwei Jahre angelegten Feldversuch liefern. Der Mautbetreiber betont, dass die Datenüberlassung vom aktuellen Mautgesetz gedeckt sei. Die Kosten des "Truck Guide Hamburg" sollen bei zwei Millionen Euro liegen und aus dem Konjunkturprogramm des Stadtstaates getragen werden.

5.2.2.2 Lkw-Maut: Rechtliche Grundlage zur Überlassung von Mautdaten fehlt

Einen Tag nach dem Erscheinen des oben zitierten Artikels, wurde seitens des Mautbetreibers bekannt, dass noch keine rechtlichen Rahmenbedingungen für solch eine Anwendung bestehen. Toll-Collect-Sprecherin Claudia Steen betonte, gegenüber „heise-online“, dass man sich aber um eine Ausnahmegenehmigung für einen Feldtest mit zirka 200 LKW bemühe, die die Bundesregierung erteilen müsse. In jedem Fall werde man alle Datenschutzrichtlinien streng beachten. Wie berichtet, soll mit Hilfe der Daten von Toll Collect der zunehmende LKW-Verkehr von und zu den Container-Terminals entzerrt werden. Gedacht ist dabei an einen sogenannten "Mehrwertdienst", der in den On-Board-Units (OBUs) von Toll Collect laufen soll. Die Container-Lkw, die den Hamburger Hafen ansteuern, sollen frühzeitig erfasst und einem Lade-Zeitfenster zugeordnet werden. Der Fahrer wird dann über die OBU informiert, wann er wo den Container ab- oder aufladen kann. Rund 40 Prozent des Containeraufkommens im Hamburger Hafen werden im weiteren Umland von Hamburg per LKW "zwischengespeichert". Die Entzerrung dieses Verkehrs könnte wesentlich zur Stauvermeidung in Hamburg beitragen.

Für Toll Collect wäre der Feldtest ein Einstieg in das Angebot von erweiterten Diensten rund um die OBU, mit der seit viereinhalb Jahren die LKW-Maut automatisch abgerechnet wird. Nach Angaben von Toll Collect sind derzeit 640.000 Fahrzeuge mit einer solchen OBU ausgestattet. Firmensprecherin Steen bestätigte,

dass es Gespräche zwischen der Hamburger Port Authority, der Softwarefirma Dakosy und dem Verband Straßengüterverkehr gibt. Es gebe allerdings noch keine Konsortialvereinbarungen zur Durchführung des Projekts. "Es fehlen nach wie vor die rechtlichen Rahmenbedingungen und die für die Durchführung eines Feldtests notwendige Zustimmung des Bundes. Beides ist in Klärung. Für alle Aktivitäten benötigen wir die Genehmigung des Bundes, erst danach können die konkreten Vorbereitungen beginnen." In jedem Fall müssten sowohl die Container-Speditionen, die am Feldtest teilnehmen wollen, als auch die Fahrer ihr Einverständnis erklären, dass sie diese Form der Auswertung von Arbeitsplatzdaten akzeptieren. In diesem Zusammenhang legt Toll Collect Wert auf die Feststellung, dass mit den derzeitigen Mautdaten Informationen über Position, Fahrtrichtung und die Geschwindigkeit von LKW noch nicht verfügbar seien (aus [6W]).

5.2.3 Fazit

Im Unterschied zu FLEET geht es hier datenschutzrechtlich gerade um die Verarbeitung personenbezogener Daten. Dem Betreiber ist es möglich, die Positions- und Zeitangaben einer natürlichen Person zuzuordnen. Die Daten, insbesondere Positions- und Zeitangaben, sind datenschutzkonform zu erheben und es ist entscheidend, dass er die Zustimmung des Betroffenen vorweg und zweifelsfrei eingeholt hat. Auf die arbeitsrechtlichen Besonderheiten in diesem Zusammenhang wie in Kapitel 2 ausführlich beschrieben, wird an dieser Stelle verwiesen.

Für die übrigen Aspekte dieses Projekts kann generell und exemplarisch auf die rechtliche Bewertung des Projekts FLEET verwiesen werden (Immaterialgüterrecht; Vertragsrecht). Im konkreten Fall werden ggf. auch fracht- bzw. speditionsrechtliche Sonderbestimmungen zu beachten sein, auf die hier nicht weiter eingegangen wird.

5.3 Das Filmen von Personen

Das Filmen von Personen, sei es im Rahmen von Kartenmaterialsammlungsaktivitäten, wie bei Google oder aus Sicherheitsgründen wie bei den Wiener Linien, ist in Österreich ein kritisches Thema. Eine Erlaubnis dafür ist bei der Datenschutzkommission einzuholen und wird in den seltensten Fällen erteilt.

5.3.1 Google Street View in Österreich

Die österreichische Datenschutzkommission hat den umstrittenen dreidimensionalen Internet-Straßenplan „Google Streetview®“ vorläufig (Ende Mai 2010) gestoppt. Das bedeutet, dass Google ab sofort keine Aufnahmen in Österreich machen und bereits vorhandene Aufzeichnungen nicht verwenden darf. Es wurde ein Prüfverfahren eingeleitet. Die umstrittenen Google-Streetview-Autos dürfen in Österreich zumindest vorläufig nicht mehr fahren.

Die österreichische Datenschutzkommission hat ein "amtswegiges" Prüfverfahren eingeleitet - hauptsächlich deshalb, weil Google weder die Aufzeichnung von WLAN-Standorten noch die Sammlung von persönlichen Daten angemeldet hatte, sagt

Waltraud Kotschy von der Datenschutzkommission. Damit sei nicht klar, wie weit die Fotoaufnahmen technisch vom Sammeln von Daten getrennt seien. Deshalb habe man vorläufig „Google Streetview“ per Bescheid untersagt. Die Verletzung der Meldepflicht ist in Österreich mit einer Strafe von bis zu 10.000 Euro bedroht. Zum Vergleich: Für Waltraud Kotschy ist dieser Fall auch Anlass dafür, das Ausmaß der Strafmöglichkeiten in Österreich zu diskutieren: Möglicherweise seien die Sanktionsmöglichkeiten bei Datenschutzverletzungen nicht ausreichend, so Kotschy (aus [3W]).

5.3.2 Google Street View in Deutschland

Das Produkt „Google Street View“ ist auch in Deutschland mehrfach heftig in die Kritik geraten. Kritikpunkt war zunächst die Verletzung des grundgesetzlich geschützten Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG).

Jüngst wurde auch noch bekannt, dass Google zusammen mit dem „Abfilmen“ von Straßenzügen auch Daten aus Funknetzen (WLAN) erfasst und gespeichert hat. Die Einzelheiten dieses Vorwurfs sind noch nicht abschließend geklärt. Infolge einer Strafanzeige ermittelt die Hamburger Staatsanwaltschaft wegen dieses Vorfalls gegen Google.

Die Sorge um die durch „Google Street View“ in den Fokus der Öffentlichkeit und der Politik getretene Datenerhebung aus dem öffentlichen Raum führte zu einem Beschluss der 81. Konferenz der Justizministerinnen und Justizminister am 23. und 24. Juni 2010. Die deutschen Justizminister halten es für erforderlich, für die Speicherung und weitere Verarbeitung personenbezogener Daten, die im Zusammenhang mit der Erfassung von Gebäuden, Straßen, Plätzen und vergleichbaren raumbezogenen Objekten und Gegenständen erhoben werden, einen wirksamen Schutz der von der Datenerhebung Betroffenen sicher zu stellen. Sie unterstützen daher einen Gesetzesantrag, wonach durch Änderungen des deutschen Bundesdatenschutzgesetzes der Schutz Betroffener vor Verletzungen ihrer Persönlichkeitsrechte verbessert werden soll. In den Beratungen über den Gesetzesantrag wird dann – so die Justizminister - zu bewerten sein, wie das Recht auf informationelle Selbstbestimmung der Betroffenen einerseits durch die Schaffung von Anonymisierungspflichten sowie andererseits eines wirksamen Widerspruchsrechts gestärkt wird. Ein konkreter Ansatz ist noch vorgestellt.

In der Sache widersprechen die Justizminister damit auch dem Ansatz, dass die bereits bestehenden Datenschutzbestimmungen einen ausreichend schützenden Rechtsrahmen böten. Dies mag auch daran liegen, dass sich im Fall von Google gezeigt hat, dass rechtlichen Maßnahmen zur Durchsetzung von Datenschutzbestimmungen bei Unternehmen mit Sitz im Ausland an seine Grenzen stößt. Ebenso wird damit deutlich, dass den Justizministern die Aussage von Google zu Selbstverpflichtungen nicht genügt (vgl.: 81. Konferenz der Justizministerinnen und Justizminister am 23. und 24. Juni 2010 in Hamburg, Beschluss, TOP I.2, (siehe [7W]).

5.3.3 Stations- und U-Bahnüberwachung der Wr. Linien

Laut einem Artikel der Wiener Zeitung vom 17.10.2009 (siehe [1W]) wurde die Stationsüberwachung der Wiener Linien mit mehr als 1100 Kameras, die bis 30. Juni 2009 befristet erlaubt war, nun von der Datenschutzkommission auf Dauer gewährt. Demnach konnten die Wr. Linien den Kamera-Einsatz durch Vorlage ausreichender Materialien rechtfertigten. Videomitschnitte aus den Stationen dürfen nun 120 Stunden gespeichert werden, bevor sie gelöscht werden müssen.

Die Wiener Linien hatten für die DSK ausreichend Material vorgelegt, die den Kamera-Einsatz rechtfertigten. Allerdings hatten die Wr. Linien auch Auflagen-Verstöße zu vertreten und Aufzeichnungen tw. unerlaubt vorgenommen, Bemerkenswert ist, dass Videoaufzeichnungen in einem arbeitsrechtlichen Verfahren gegen einen Mitarbeiter der Wiener Linien verwendet werden sollten.

Zu den Grundsätzen der Videoüberwachung wird auf Kapitel 2 Exkurs: Videoüberwachung verwiesen.

Weiter befristet bleibt hingegen die Videoüberwachung in U-Bahn-Zügen und Straßenbahnen. Hier ist die Lizenz zur Datenspeicherung mit 30.12.2011 begrenzt.

6. Handlungsempfehlungen

Aus den obigen Erläuterungen und Analysen ergeben sich für die Verkehrstelematik folgende Handlungsempfehlungen in Hinsicht auf deren Rechtsaspekte:

- Allfällige datenschutzrechtliche Probleme müssen bereits zu Projektbeginn (bzw. davor) angedacht und genauestens analysiert werden, da sie sich als Showstopper erweisen können. Wenn das Produkt bzw. die Dienstleistung fertig entwickelt wurde, ist es oft zu spät.
- In Teststellungen gelten dieselben datenschutzrechtlichen Bedingungen wie im Regelbetrieb!
- Eine wichtige Frage, die man sich jedenfalls im Zusammenhang mit dem Datenschutz stellen sollte ist: „Benötige ich in meinem Projekt wirklich personenbezogene Daten?“ Wird die Frage bejaht, kann dies das Projekt komplexer oder gar unmöglich machen.
- Die Bestimmungen zur Videoüberwachung sind auch nach der Novelle des DSG in vielen Fällen stark einschränkend, insofern sie eine Videoüberwachung im öffentlichen Raum nur sehr eingeschränkt ermöglichen.
- Das Immaterialgüterrecht ist ausreichend, um gegenwärtige und zukünftige Telematikanwendungen entwickeln und implementieren zu können.
- Bei der Teilnahme mehrerer Personen an einem Telematikprojekt muss immaterialgüterrechtlich auf die Frage der Verwertungsrechte Bedacht genommen werden. Ein eigenes Telematikgesetz ist aus Sicht der Projektgruppe nicht notwendig. Abgesehen von den einzelnen Einschränkungen im Bereich des Datenschutzes sind die rechtlichen Grundlagen in der österreichischen Rechtsordnung ausreichend für die Entwicklung und Implementierung von Telematikprojekten.
- Ein Defizit besteht heute etwa darin, dass für die Videoüberwachung von Schutzwegen in der STVO keine rechtliche Grundlage besteht. Für die Videoüberwachung von neuralgischen Eisenbahnkreuzungen wurde erst jüngst im Eisenbahngesetz eine ausreichende Grundlage geschaffen.

Allerdings ist aufgrund der regelmäßigen Involvierung mehrerer Beteiligter in Telematikprojekten auf eine detaillierte vertragliche Ausgestaltung der Beziehungen der Beteiligten besonderer Wert zu legen, da das dispositive österreichische Zivilrecht oftmals keine eindeutige Rechtsfolge beinhalten wird. Insbesondere die Leistungsbeschreibung, Quality of Service-Normen und Haftungsbestimmungen bedürfen einer exakten fallspezifischen Ausarbeitung.

7. Conclusio

Zusammenfassend kann gesagt werden, dass in Österreich vor allem die Bestimmungen zum Datenschutz die technischen Möglichkeiten von Verkehrstelematikprojekten zu Gunsten des Grundrechtschutzes von Betroffenen einschränken. Demgegenüber stehen neue Entwicklungen, wie die Videoüberwachung von Schutzwegen, für die es derzeit keine Rechtsgrundlagen gibt. Der Einbezug der rechtlichen Bestimmungen muss aber jedenfalls rechtzeitig angedacht und umgesetzt werden, um Produkte oder Dienstleistungen schlussendlich erfolgreich auf den Markt überleiten zu können.

Literaturverzeichnis

ABC Consulting, AIT. (2010). Projektvorschlag: Automatische videobasierte Verkehrsanalyse im Bereich eines Schutzweges. Wien
AIT (2004). FLEET_Endbericht_V5.doc
AIT (2007). Endbericht_GO-SMART_V1-0 FINAL.doc
Ambrosch, K. E. (2008). *Intelligent transport systems — System architecture — Privacy aspect in ITS standards and systems.* Genf: ISO Copyright Office.
ARGE DoRIS. (2005). *Rechtliche Rahmenbedingungen für den Betrieb von River Information Services.* Wien: bmvit
Chloupek, Alexander. (2010). *Vorlesungsunterlagen zum Gastvortrag „Telematik im Schienenverkehr“ im Rahmen der Schienenverkehrsvorlesung an der FH des bfi Wien*.
COMMUNICATION FROM THE COMMISSION. (2007). *Freight Transport Logistics Action Plan*
COMMUNICATION FROM THE COMMISSION. (2008). *Action Plan for the Deployment of Intelligent Transport Systems in Europe*
Lange, M. (2008). *Redlight Enforcement an Eisenbahnkreuzungen.* Wien
Morawetz, K. (2010). *Erfolgreiche Einführung von Technologieentwicklungen für Intelligente Verkehrs- und Transportsysteme am Markt.* Wien: FH Technikum Wien.
SLR Engineering OG. (2010). *PD2010 - Pedestrian Detection Infofolder*. Graz
Taeger, J., & Wiebe, A. (2005). *Mobilität Telematik Recht.* Köln: Dr. Otto Schmidt.
Wissenschaftliches Redaktionskomitee der OCG. (2007). *Österreichisches Informationssicherheitshandbuch Teil I und Teil II.* Wien.
World Road Association (PIARC). (2004). *The Intelligent Transport Systems Handbook (2nd Edition).* Swanley (Kent), United Kingdom: Route One Publishing.

Rechtsgrundlagen

Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz - **ArbVG**). StF: BGBl. Nr. 22/1974
Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - **DSG** 2000) .StF: BGBl. I Nr. 165/1999
Bundesgesetz über Eisenbahnen, Schienenfahrzeuge auf Eisenbahnen und den Verkehr auf Eisenbahnen (Eisenbahngesetz 1957 - **EisbG**) .StF: BGBl. Nr. 60/1957
Bundesgesetz über eine umweltrelevante Geodateninfrastruktur des Bundes (Geodateninfrastrukturgesetz – **GeoDIG**). StF: BGBl. I Nr. 14/2010
Bundesgesetz vom 23. Juni 1967 über das Kraftfahrwesen (Kraftfahrgesetz 1967 - **KFG**. 1967). StF: BGBl. Nr. 267/1967
Patentgesetz 1970 – **PatentG**. StF: BGBl. Nr. 259/1970 (WV)
Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - **SPG**). StF: BGBl. Nr. 566/1991
Bundesgesetz vom 6. Juli 1960, mit dem Vorschriften über die Straßenpolizei erlassen werden (Straßenverkehrsordnung 1960 - **StVO**. 1960). StF: BGBl. Nr. 159/1960
Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - **TKG** 2003). Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird und das Bundesgesetz über die Verkehrs-Arbeitsinspektion und das KommAustria-Gesetz geändert werden. StF: BGBl. I Nr. 70/2003
Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz) – **UrhG** Stand 2010. StF: BGBl. Nr. 111/1936

Internetquellen

[1W]	http://2005.wienerzeitung.at/DesktopDefault.aspx?TabID=5067&Alias=wzo&cob=444992&Page17212=22
[2W]	http://futurezone.orf.at/stories/1604827/
[3W]	http://oe1.orf.at/artikel/245782
[4W]	http://www.cargomon.com/
[5W]	http://www.heise.de/newsticker/meldung/142952
[6W]	http://www.heise.de/newsticker/meldung/143044
[7W]	http://www.justiz.nrw.de/JM/justizpolitik/jumiko/beschluesse/2010/fruehjahrskonferenz10/I_2.pdf

Abbildungsverzeichnis

Abbildung 2-1: Projektschwerpunkte 11
Abbildung 4-1: Systemübersicht FLEET 37
Abbildung 4-2: Systemübersicht GO-Smart 42
Abbildung 4-3: Systemskizze Red Light Enforcement an Eisenbahnkreuzungen 45
Abbildung 4-4: Pedestrian Detection (Quelle: SLR engineering OG) 47
Abbildung 4-5: Standorte Kamerasysteme Schutzwegüberwachung 48
Abbildung 4-6: CargoObserver MTU 52
Abbildung 4-7: Einsatz CargoObserver 53
Abbildung 4-8: Taktisches Verkehrsbild DoRIS 55
Abbildung 4-9: DoRIS Basisstationen in Österreich 55

Tabellenverzeichnis

Tabelle 4-1: Einsatzbereiche der Telematik im Straßenverkehr (Quelle: ITS Handbuch, erweitert durch das Projektteam) 36
Tabelle 4-2: Einsatzbereich der Telematik im Schienenverkehr (Quelle: Lehrunterlagen DI Alexander Chloupek) 49
Tabelle 4-3: Einsatzbereiche der Telematik in der Schifffahrt 54
Tabelle 4-4: Einsatzbereiche der Telematik in der Luftfahrt (Quelle: Austro Control, erweitert durch das Projektteam) 56

Abkürzungsverzeichnis

ADAS	Advanced Driving Assistance Systems
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AIS	Automatic Identification System-Transponder
ArbVG	Arbeitsverfassungsgesetz
BDSG	Bundesdatenschutzgesetz (D)
DoRIS	Danube River Information Service
DSG 2000	Datenschutzgesetz 2000 (Ö)
DSRC	Dedicated Short Range Communication
EBuLA	Elektronischer Buchfahrplan und Langsamfahrstellen
EETS	European Electronic Toll Service
FCD	Floating Car Data
FLEET	Fleet Logistics Service Enhancement with Egnos & Galileo Satellite Technology
GeoZG	Geodatenzugangsgesetz
GPS	Global Positioning System
hzG	Höchst zulässiges Gesamtgewicht
INSPIRE	Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14.03.2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft
ITS	Intelligent Transport Systems
I2M	Inbound to Manufacturing
IWG	Informationsweitergabegesetz
JUERGEN	Juristische Rahmenbedingungen für die Erfassung, Verarbeitung, Verbreitung und Benutzung von intermodalen Verkehrsinformationen durch Dritte für Mobilitätsinformationsdienstleistungen.
Kfz	Kraftfahrzeug
LKW	Lastkraftwagen
MTU	Master Telematics Unit
ÖBB	Österreichische Bundesbahnen
OBU	On-Board-Unit
ÖPNV	Öffentlicher Personennahverkehr

ÖV	Öffentlicher Verkehr
PatG	Patentgesetz (D)
PatentG	Patengesetz (Ö)
PIARC	World Road Association
RIS	River Information Service
RFID	Radio Frequency Identification
SIL	Sicherheitslevel
SMS	Short Message Service
SPG	Sicherheitspolizeigesetz
STMV 2000	Standard- und Musterverordnung 2000
StVO	Straßenverkehrsordnung
SU	Sensor Unit
TKG	Telekommunikationsgesetz (2003)
TMC	Traffic Message Channel
TMG	Telemediengesetz
UGB	Unternehmensgesetzbuch
UrhG	Urheberrechtsgesetz
VIONA	Video Identifikation und Online Analysen für den motorisierten Individualverkehr