Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK

Externe Benutzer ME

Katja Gysin, 30. November 2020

Datenschutz Mobilitätsdaten

Bericht

Dokumentennummer: ASTRA-D-DB3D3401/359

Impressum

Erstelldatum / Revisionsdatum:	30.11.2020
Ersteller/in:	Gyk
Verzeichnis / Dateiname:	2020-11-30 Bericht Datenschutz Mobilitätsdaten.docx
Anzahl Seiten:	19
Genehmigt am:	
Genehmigt von:	Wie

Änderungsverzeichnis

Version	Datum	Ersteller	Bemerkungen
0.9	30.11.2020	Gyk	Entwurf zur Freigabe Wie
1.0	25.02.2021	Gyk	Finale Version

Inhaltsverzeichnis

1. Einführung

Wenn wir von Datenschutz reden, müssen wir uns zuerst einig sein, was wir darunter verstehen. Datenschutz im strikt rechtlichen Sinn avisiert den Persönlichkeitsschutz. Das Grundrecht auf informationelle Selbstbestimmung schafft den Anspruch, dass jede Person selber bestimmen kann, ob und zu welchem Zweck Informationen über sie gespeichert und bearbeitet werden.

Die Regeln für den generellen Umgang mit Personendaten finden sich in den Datenschutzgesetzen und in Sachgesetzen, die insbesondere den Zweck von konkreten Datenbearbeitungen festlegen. Von Datenschutz sprechen wir aber nur, wenn es sich bei den fraglichen Daten um Angaben zu einer Person handelt. Werden Sachdaten – also Daten ohne Personenbezug – bearbeitet, kommen die Vorgaben des Datenschutzes nicht zur Anwendung. Was es aber auch in diesem Bereich braucht, sind Massnahmen der Informationssicherheit, um die Daten zu schützen. Die Abgrenzung von Personen- und Sachdaten ist dabei weniger offensichtlich als es scheinen mag. Spezifische datenschutzrechtliche Herausforderungen im Bereich der Mobilität stellen sich aber auch in der Identifikation von Risiken und der Zuordnung von Verantwortlichkeiten.

Ziel des Berichtes ist es, eine Übersicht zu den Grundlagen des Datenschutzes, zu den datenschutzrechtlichen Prinzipien und den datenschutzrechtlichen Risiken von Mobilitätsdaten zu schaffen. Der Bogen wird dabei bewusst weit gespannt und es werden Fragen der multimodalen Mobilität, insbesondere die Zurverfügungstellung von Daten zur Verbesserung von Mobilitätsangeboten, wie auch Fragen der automatisierten Fahrzeuge und des vernetzten Verkehrs behandelt. Dieser Überblick soll eine gemeinsame Grundlage und auch Sprache für die weiteren Arbeitsschritte bereitstellen. Er wird aber noch nicht konkrete Antworten auf spezifische Fragen aus mobilitätsrelevanten Projekten liefern können. Dies wird in den folgenden Konkretisierungsschritten – siehe auch die Schlussfolgerungen – gemacht werden müssen.

Der Berichtsentwurf wurde sowohl in der Kerngruppe Intelligente Mobilität – einem ASTRA-internen Gremium – vorgestellt, wie auch im Fachausschuss multimodale Mobilität präsentiert. Im Fachausschuss mmM sind die folgenden Ämter vertreten: BAV, swisstopo, BfS, ARE, BFE, BAKOM und natürlich das ASTRA. Der Bericht wurde auch dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vorgelegt. Die Rückmeldungen aus den verschiedenen Gremien haben bereits in den Bericht Eingang gefunden und sind Teil der Projektdokumentation.

1.1 Anwendung Datenschutzrecht

Vereinfacht gesagt, kommt Datenschutzrecht dann zur Anwendung, wenn «jemand Personendaten bearbeitet»:

1. **Jemand** kann eine private Person, ein privates Unternehmen oder eine staatliche Institution auf kommunaler, kantonaler oder Bundesebene sein.
2. **Bearbeiten** heisst sichten, erheben, erfassen, organisieren, ordnen, speichern, verändern, auslesen, abfragen, verwenden, offenlegen, verknüpfen, löschen, vernichten – eigentlich jeder Umgang mit Personendaten.
3. **Personendaten** sind gemäss Definition in Art. 3 des Datenschutzgesetzes: «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen». Alle anderen Daten sind grundsätzlich Sachdaten.

Insbesondere die Abgrenzung von Personen- und Sachdaten ist alles andere als trivial (dazu unten mehr). Sie ist aber zentral bei der Bestimmung, ob Datenschutzrecht und damit die nachstehend angeführten Vorgaben überhaupt zur Anwendung kommen. Bei der Bearbeitung von Sachdaten sind Fragen der Verantwortlichkeit oder Vorgaben zur Informationssicherheit nicht zu unterschätzen.

Exkurs Personendaten

Bestimmbarkeit

Eine Person ist *bestimmt*, wenn sich ihre Identität unmittelbar aus den Daten selbst ergibt, z.B. durch den Namen. Eine Person ist *bestimmbar*, wenn sich ihre Identität aus dem Kontext der Daten oder durch Kombination mit anderen Daten ergibt, solange dies ohne unverhältnismässigen Aufwand möglich ist. Unverhältnismässig ist der Aufwand, wenn nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass jemand diesen auf sich nehmen wird. Beim Aufwand sind auch die technischen Möglichkeiten zu berücksichtigen. Gesichtserkennungssoftware erlaubt beispielsweise die Zuordnung einer Identität zu einem Foto, auch wenn jemand die Person nicht kennt. Dabei ist nicht nur der objektiv erforderliche Aufwand relevant, sondern auch das Interesse, das jemand an der Identifizierung hat. Die Bestimmbarkeit ist somit relativ: Eine Person kann für jemanden aufgrund seines Wissen oder der zur Verfügung stehenden Möglichkeiten bestimmbar sein, für andere aber nicht. Und ein und dieselbe Angabe kann – je nach Kontext, Zweck der Datenbearbeitung und bearbeitender Person – einmal ein Personendatum sein und ein andermal nicht. Die Autohalterin ist bestimmt durch die Eintragung im Fahrzeugausweis, aber auch durch eine Halterabfrage über das Nummernschild des Autos. Je nach Möglichkeiten und Zusatzinformationen, die jemand hat, ist sie somit über das eine oder andere Mittel identifizierbar.

Anonymisierung / Pseudonymisierung

Nicht mehr bestimmbar ist eine Person, wenn Personendaten anonymisiert werden. Dabei wird der Personenbezug so aufgehoben, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr möglich sind. Anders als bei der Pseudonymisierung darf kein Schlüssel aufbewahrt werden, der die Re-Identifikation der betroffenen Person ermöglicht. Pseudonymisierte Personendaten bleiben Personendaten für alle, die den Zugang zum Schlüssel haben. Für Aussenstehende können pseudonymisierte Personendaten als anonymisiert betrachtet werden. Anonymisierte Daten sind den Sachdaten gleichzustellen und fallen ausserhalb des Anwendungsbereichs des Datenschutzrechts.[1]

«Gewöhnliche» und besonders schützenswerte Personendaten

Je nach Art der bearbeiteten Daten gelten unterschiedliche Anforderungen. Das Gesetz (Art. 3 lit. c DSG) definiert als besonders schützenswerte Personendaten die religiöse, weltanschauliche, politische oder gewerkschaftliche Ansicht oder Tätigkeit; die Gesundheit, die Intimsphäre und die Rassenzugehörigkeit (im Vorentwurf zum neuen Datenschutzgesetz – VE-DSG – wird zusätzlich auch die ethnische Herkunft ins Gesetz aufgenommen); Massnahmen der sozialen Hilfe und administrative oder strafrechtliche Verfolgungen und Sanktionen. Als besonders schützenswerte Personendaten gelten somit Angaben, bei denen eine erhöhte Gefahr einer Persönlichkeitsverletzung besteht, weil sie Ansehen oder soziale Geltung wesentlich beeinflussen und in ausgeprägtem Mass diskriminierende oder stigmatisierende Wirkung haben. Den besonders schützenswerten Daten gleichgestellt ist das Persönlichkeitsprofil, d.h. die Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit erlaubt. Hier geht es um an sich nicht sensitive Daten, die aber durch ihre Zusammenführung eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlauben können. Der VE-DSG will das Persönlichkeitsprofil durch den Begriff Profiling ersetzen, der eine bestimmte Form der Datenbearbeitung beschreibt, nämlich die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten. Damit können beispielsweise die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit oder die Mobilität analysiert und vorhergesagt werden. Die genaue Ausgestaltung des Begriffs «Profiling» und den rechtlichen Folgen waren im Parlament umstritten.

Im VE-DSG werden neu auch genetische (Information über das Erbgut einer Person) und biometrische Daten (z.B. der digitale Fingerabdruck, Gesichtserkennung, Bilder der Iris), die ein Individuum eindeutig identifizieren, als besonders schützenswerte Personendaten aufgenommen.

[1] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 7019): «Das Gesetz gilt nicht für anonymisierte Daten, wenn eine Re-identifizierung durch Dritte unmöglich ist (die Daten wurden vollständig und endgültig anonymisiert) oder wenn dies nur mit einem hohen Aufwand möglich wäre, den kein Interessent auf sich nehmen würde. Das gilt ebenfalls für pseudonymisierte Daten. »

Alle anderen Daten gelten als «gewöhnliche» Personendaten.

1.2 Abgrenzung Informationssicherheit

In der öffentlichen Wahrnehmung geht es beim Datenschutz oft auch um Cyber Security oder Datensicherheit. Datenschutz und Datensicherheit stehen zwar in einer Wechselwirkung, sind aber voneinander abzugrenzen. Beim Datenschutz geht es um den Persönlichkeitsschutz des Einzelnen. Die Datensicherheit zielt hingegen generell auf die bei einem Verantwortlichen vorhandenen Daten ab – Sach- oder Personendaten – und umfasst den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung. Sie ist ein integraler Bestandteil des Datenschutzes, geht aber auch weiter, da damit auch Sachdaten oder Geschäftsgeheimnisse geschützt werden können.

1.3 «Privacy paradox»

In der Diskussion um den Datenschutz geht es oft auch mehr um den «gefühlten» als um den rechtlichen Datenschutz. Damit ist das Unbehagen von Menschen in Bezug auf den Umgang mit Daten durch Staatsorgane oder private Unternehmen gemeint. Es geht um die Frage, wie Betroffene eine Datenbearbeitung wahrnehmen und wie hoch das Missbrauchspotential eingeschätzt wird. Je unsicherer Menschen mit der Anwendung sind, desto weniger werden sie genutzt. Das Beispiel der Covid-App hat diese Diskussionen sehr schön aufgezeigt.

In eine ähnliche Richtung zielt der Begriff «privacy paradox». Damit ist der Widerspruch zwischen dem sorglosen Verhalten beim Umgang mit den eigenen Personendaten und der gleichzeitigen Sorge über die mangelnde Privatsphäre gemeint. Dienste werden genutzt, obwohl die Menschen kein volles Vertrauen in sie haben, und auch wenn Menschen sagen, dass ihnen Privatsphäre wichtig ist, handeln sie nicht immer entsprechend. Ist der eigene Vorteil oder die Bequemlichkeit eines Angebots hoch genug, wird die Nutzung der Daten durch Dritte häufig stillschweigend in Kauf genommen. Hier spielt natürlich auch eine Rolle, dass es für den Einzelnen kaum sichtbar ist, was mit seinen Daten geschieht und ihm momentan zumindest kein Nachteil entsteht. Der Nutzen ist oft unmittelbarer als die Kosten, die erst ex post wahrgenommen werden. Es ist aber auch festzuhalten, dass die Gesellschaft in Bezug auf ihre Wahrnehmung, was Digitalisierung bedeutet, noch in den Kinderschuhen steckt. Der gesellschaftliche Dialog, was Digitalisierung sollen kann und nicht einfach was sie kann, beginnt erst und wird wohl noch einige Stadien durchlaufen.

Im Hinblick auf die Schaffung neuer Datenräume oder Instrumente, die Daten benötigen um zu funktionieren, scheint es gerade aus staatlicher Sicht grundlegend, dass die Nutzung von Daten in transparenter Weise geschieht. Die Datenschutzgesetzgebung setzt dies als Grundlage für die Datenbearbeitung voraus.

1.4 Digitale Selbstbestimmung

In diese Richtung zielt die unter der Federführung des BAKOM lancierte Initiative «Netzwerk Digitale Selbstbestimmung».[2] Die Strategie Digitale Schweiz postuliert, dass sich die Schweiz für eine partizipative Digitalisierung einsetzt, in der die Menschen und ihre digitale Selbstbestimmung im Zentrum stehen. Die digitale Selbstbestimmung soll Bürgerinnen und Bürger befähigen, über ihr Leben im digitalen Raum selbst zu bestimmen. Die Teilhabe an der digitalen Welt soll nicht mehr mit einem Kontrollverlust über die eigenen Daten assoziiert werden. Dafür braucht es neue Strukturen, die dem Einzelnen eine aktive Steuerung der digitalen Transformation ermöglichen.

Gemeinsame Datenräume können einen Mehrwert schaffen, indem sie die Nutzung von Daten über ihren ursprünglichen Verwendungszweck hinaus und neue Formen der gemeinsamen Nutzung ermöglichen. Ein solcher Datenraum basiert auf verankerten Rechten, verbindlichen Regeln und Normen sowie gemeinsamen technischen und organisatorischen Infrastrukturen. Datenräume können auf regionaler, nationaler und internationaler Ebene entstehen und die Datennutzung in einem bestimmten Wirtschaftssektor oder über die Grenzen einzelner Sektoren hinaus umfassen. Die Schweiz soll den Zugang zu vertrauenswürdigen Datenräumen für Personen, Unternehmen und den öffentlichen Sektor fördern.

[2] Non Paper Digitale Selbstbestimmung, Stand 15.05.2020

Zu diesem Zweck erarbeiten das BAKOM und die Direktion für Völkerrecht im EDA zusammen mit weiteren Akteuren bis Ende 2021 einen Grundlagenbericht, der aufzeigen wird, wo für den Staat Handlungsbedarf besteht.

2. Rechtmässigkeit der Datenbearbeitung

Personendaten dürfen nur rechtmässig bearbeitet werden. Voraussetzung für eine rechtmässige Bearbeitung oder Nutzung personenbezogener Daten ist eine rechtlich einwandfreie Erhebung dieser Daten. Die Grundsätze von Art. 4 und 5 des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) müssen bei jeder Datenbearbeitung respektiert werden. Dazu gehört die Bearbeitung nach Treu und Glauben, die Verhältnismässigkeit, die Zweckbindung und die Regeln der Transparenz. Wird gegen diese Grundsätze verstossen, wird die Persönlichkeit der betroffenen Personen verletzt. Dies kann nur erlaubt sein, wenn ein Rechtfertigungsgrund vorliegt. Das kann die Einwilligung, ein überwiegendes privates oder öffentliches Interesse oder das Gesetz sein (Art. 13 DSG). Ein überwiegendes privates Interesse kann beispielsweise eine vertragliche Vereinbarung sein.

Bei Bundesorganen (wie auch bei kantonalen oder kommunalen öffentlichen Organen) gilt das Legalitätsprinzip, d.h. jedes Handeln beruht auf einer entsprechenden gesetzlichen Grundlage. Das kann eine Bestimmung in einem Bundesgesetz, einer Verordnung oder auch einem kantonalen bzw. kommunalen Gesetz oder Verordnung sein. Es kann auch eine rechtliche Vorgabe auf internationaler oder europäischer Stufe sein, soweit sie für die Schweiz oder ein Schweizer Unternehmen anwendbar ist.

Auch private Personen oder Unternehmen können sie sich auf eine gesetzliche Grundlage stützen für ihre Datenbearbeitung, z.B. private Versicherungsunternehmen gestützt auf die Versicherungspflicht von Art. 63 SVG. Im Regelfall bearbeiten Private aber Personendaten gestützt auf die Einwilligung der betroffenen Person (Art. 13 Abs. 1 i.V.m. Art. 4 Abs. 5 DSG).

Exkurs Datenschutzrecht – Hierarchie

Bund

Auf Bundesebene ist der Datenschutz gegenwärtig primär im Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) geregelt, das am 1. Juli 1993 in Kraft getreten ist. Das DSG regelt die Bearbeitung von Daten natürlicher und juristischer Personen durch private Personen und durch Bundesorgane und enthält Grundsätze, die beim Bearbeiten von Daten zu befolgen sind. Neben dem DSG gelten in vielen Bereichen Spezialgesetze, die ebenfalls datenschutzrechtliche Bestimmungen enthalten (bereichsspezifische Datenschutznormen).

Das DSG wurde revidiert um einerseits Schwächen zu beheben, die aufgrund der rasanten technologischen Entwicklung entstanden sind; andererseits soll die Revision den Entwicklungen auf der Ebene des Europarats und der Europäischen Union Rechnung tragen. Das revidierte Gesetz wurde in der Herbstsession 2020 des Parlaments verabschiedet; wann es in Kraft tritt, steht noch nicht fest.

Europäische Union (EU)

Die EU hat im April 2016 eine Reform der Datenschutzgesetzgebung verabschiedet, die zwei Erlasse umfasst. Dabei handelt es sich erstens um die Datenschutz-Grundverordnung (DSGVO, Verordnung (EU) 2016/679), welche die bisherige Richtlinie 95/46/EG ersetzt hat. Die DSGVO ist in den EU-Mitgliedstaaten seit Mai 2018 direkt anwendbar. Der zweite verabschiedete Erlass ist die Richtlinie (EU) 2016/680, die den Rahmenbeschluss 2008/977 /JI ersetzen wird.

Für die Schweiz ist Letztere Bestandteil des Schengen-Acquis. Aufgrund des Schengen-Assoziierungsabkommens muss die Schweiz die Richtlinie umsetzen. Sie hat dies mit dem Erlass des Schengen-Datenschutzgesetzes 2018 gemacht. Hingegen ist sie nicht verpflichtet, die DSGVO zu übernehmen, da es sich hier nicht um eine Weiterentwicklung des Schengen-Acquis handelt.

Nichtsdestotrotz hat die DSGVO eine starke Wirkung auf die Entwicklung des Datenschutzrechts auch in der Schweiz. Zum einen dürfen Daten zwischen einem Drittstaat wie der Schweiz und EU-Mitgliedstaaten nur ausgetauscht werden, wenn der Drittstaat ein angemessenes Schutzniveau gewährleistet. Die EU wird dies in einem Angemessenheitsbeschluss – der noch dieses Jahr erwartet wird – entscheiden. Voraussetzung dafür ist, dass die schweizerische Gesetzgebung einen den Anforderungen der DSGVO entsprechenden Schutz gewährleistet. Zum andern postuliert die DSGVO eine extraterritoriale Anwendung, die auch Schweizer Unternehmen betrifft, wenn sie Personen in der EU Waren oder Dienstleistungen anbieten. Darüber hinaus hat die DSGVO eine Signalkraft weit über ihren eigentlichen Anwendungsbereich hinaus und setzt heute den weltweiten Standard für die datenschutzkonforme Bearbeitung von Personendaten.

Europarat

Bereits 1981 hat der Europarat den ersten völkerrechtlichen Vertrag im Bereich des Datenschutzes verabschiedet: das Übereinkommen SEV 108, das von der Schweiz 1997 ratifiziert wurde. Das Übereinkommen SEV 108 wurde in den letzten Jahren entlang den gleichen Linien wie die DSGVO überarbeitet. Der Bundesrat hat im Oktober 2019 beschlossen, die neue Datenschutzkonvention zu unterzeichnen. Für die Ratifikation braucht es noch die Zustimmung des Parlaments. Sie ist auch für die Kantone verbindlich, die die neuen Anforderungen in ihr Recht umzusetzen müssen.

Kantone

Im Bereich des Datenschutzes hat der Bund keine generelle Rechtssetzungsbefugnis, weshalb alle Kantone ihr eigenes Datenschutzrecht erlassen haben. Der Bund regelt in seiner Gesetzgebung die Datenbearbeitung durch Bundesorgane und durch private Personen. Den Kantonen bleibt die Regelung der Datenbearbeitung durch kantonale oder kommunale öffentliche Organe.

3. Prinzipien des Datenschutzes

Die folgenden Prinzipien finden sich generell in Datenschutzregelungen, sei es auf internationaler oder europäischer Ebene, beim Bund und in den kantonalen Datenschutzgesetzen. Bei der Beurteilung der Rechtmässigkeit einer Datenbearbeitung müssen diese Grundsätze geprüft werden.

3.1 Verhältnismässigkeit

Die Bearbeitung von Personendaten muss verhältnismässig sein. Das bedeutet, dass die Datenbearbeitung zur Erreichung des gewünschten Zwecks geeignet (z.B. nicht am Zweck vorbeischiesst) und erforderlich (ohne die Daten geht es nicht). Zudem muss sie der von der Bearbeitung betroffenen Person zugemutet werden können. Die Prinzipien der Datenvermeidung und der Datensparsamkeit («nur so viel wie nötig») sind Ausdruck der Verhältnismässigkeit bei IT-Systemen.

3.2 Zweckbindung

Nach Art. 4 Abs. 3 DSG dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Der Zweck einer Datenbearbeitung ergibt sich oft aus der Rechtfertigung, also insbesondere aus der gesetzlichen Grundlage oder dem Umfang einer Einwilligung. Die Datenbeschaffung auf Vorrat, ohne konkreten Plan für deren Verwendung, ist somit nicht rechtens. Insbesondere bei der Einwilligung von Privatpersonen ist darauf zu achten, dass die Einwilligung gemäss den Regeln eingeholt wurde (Art. 4 Abs. 5 DSG – vorgängig und «nach angemessener Information freiwillig»).

3.3 Transparenz

Unabhängig von der Rechtfertigung für die Datenbearbeitung, soll die betroffene Person transparent über die Beschaffung von Personendaten informiert werden. Dabei soll nicht nur über die Beschaffung an sich informiert werden, sondern auch warum die Daten beschafft werden (Zweck), wer sie beschafft

(Identität des Verantwortlichen) und an wen die Daten eventuell weitergegeben werden (Bekanntgabe). Je komplexer eine Transaktion ist und je länger die Daten bearbeitet werden, desto höher sind die Anforderungen an die Erkennbarkeit der Beschaffung. Die Transparenz der Beschaffung und die Information der betroffenen Person bilden den eigentlichen Eckpfeiler des ganzen Datenschutzsystems.[3]

3.4 Rechte der Betroffenen

Es besteht sowohl ein Auskunftsrecht (welche Daten werden über mich bearbeitet?) wie auch einen Anspruch auf Berichtigung, Löschung, Verbot der Bearbeitung oder der Bekanntgabe an Dritte, wenn die entsprechenden Voraussetzungen bestehen, u.a. wenn die Bearbeitung widerrechtlich ist.

3.5 Informationssicherheit

Wie eingangs bereits erwähnt, kommt der Informationssicherheit bei jeder Datenbearbeitung eine immer grössere Rolle zu. Die Datenschutzgesetzgebung ist zwar jeweils technikneutral formuliert, legt aber fest, dass die Datensicherheit vom Verantwortlichen mit «angemessenen technischen und organisatorischen Massnahmen» sichergestellt werden muss. Diese Massnahmen fokussieren auf die Schutzziele der Vertraulichkeit, der Verfügbarkeit und der Integrität. Das heisst, die Massnahmen sollen sicherstellen, dass nur berechtigte Personen auf die Daten zugreifen können, dass die Daten vorhanden sind und dass sie richtig und vollständig sind. Die Verordnung zum DSG nennt folgende Risiken, gegen die ein System geschützt werden muss: Vernichtung, Verlust, technische Fehler, Diebstahl, Fälschung, unbefugtes Ändern oder Kopieren etc. (Art. 8 VDSG). Die eigentlichen Massnahmen werden nicht im Gesetz festgelegt, sondern müssen in einer individuellen Risikoanalyse erarbeitet werden. Sie sind unterschiedlich je nach Zweck, Art und Umfang der Datenbearbeitung und hängen vom Risiko und dem gegenwärtigen Stand der Technik ab. Grundsätzlich gilt, je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen.

3.6 “Privacy by design” / “privacy by default”

Diese beiden Begriffe werden mit der Revision des Datenschutzgesetzes neu eingeführt (Art. 6 VE-DSG). Datenschutz durch Technik («privacy by design») soll rechtliche Vorgaben unterstützen bzw. deren Einhaltung mit technischen Mitteln sicherzustellen, indem technische Vorkehren einen Verstoss gegen Datenschutzvorschriften bestenfalls bereits verunmöglichen. Gewisse Massnahmen wie beispielsweise die Anonymisierung von Daten können sowohl bei der Informationssicherheit wie auch bei der datenschutzfreundlichen Technik relevant sein. Die Zielrichtung der beiden Bestimmungen sind aber nicht deckungsgleich; die Datensicherheit schreibt den Verantwortlichen eine Sicherheitsarchitektur vor, wohingegen der Datenschutz durch Technik darauf abzielt, die Datenschutzvorschriften einzuhalten, z.B. sicherzustellen, dass eine Datenbearbeitung verhältnismässig ist. Weitere Massnahmen sind beispielsweise die Datenminimierung, d.h. die Datenbearbeitung wird bereits von Beginn weg so angelegt, dass möglichst wenige Daten anfallen oder diese nur für kurze Zeit aufbewahrt werden.

Ein analoges Ziel verfolgen die datenschutzfreundlichen Voreinstellungen («privacy by default»). Mittels geeigneten Voreinstellungen wird sichergestellt, dass so wenige Personendaten bearbeitet werden, wie dies im Hinblick auf den Verwendungszweck nötig ist. Datenschutzfreundliche Voreinstellungen können – entgegen Massnahmen in der Systemarchitektur – vom Einzelnen aber geändert werden und zum Beispiel grosszügiger eingestellt werden (Erweiterung der Einwilligung).

3.7 Aufbewahrung / Löschung

Ein weiterer Grundsatz des Datenschutzes besagt, dass Daten vernichtet werden müssen, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Die Verpflichtung ergibt sich auch aus dem allgemeinen Verhältnismässigkeitsgrundsatz. Die Einhaltung dieser Verpflichtung bedingt, dass der Verantwortliche Aufbewahrungsfristen festlegt, soweit das Gesetz keine spezifische Aufbewahrungsfrist vorschreibt, wie beispielsweise in Art. 958*f* OR für die 10-jährige Aufbewahrungsfrist von Geschäftsbüchern.

[3] Botschaft zur Änderung des DSG, BBl 2003 2126

4. Verantwortlichkeit

Verantwortlich für die Einhaltung des Datenschutzes und damit auch für die Sicherstellung, dass oben ausgeführte Prinzipien respektiert werden, ist die private Person oder das Bundesorgan, die oder das über den Zweck, die Mittel und den Umfang der Bearbeitung von Daten entscheidet. Die Begrifflichkeit wird im VE-DSG den europäischen Vorgaben angepasst, bis jetzt spricht das DSG vom «Inhaber der Datensammlung». Damit es sich um einen «Verantwortlichen» handelt, müssen somit zwei kumulative Kriterien erfüllt sein: Der Datenbearbeiter bestimmt den Zweck der Bearbeitung und hat die Mittel für die Bearbeitung unter seiner Kontrolle. Die Bestimmung des Verantwortlichen ist in der Realität nicht immer einfach. Es kann durchaus mehrere Verantwortliche geben, die sich Aufgaben und Kompetenzen teilen.

Exkurs – Datenhoheit und Dateneigentum

Datenhoheit wie auch Dateneigentum sind keine rechtlichen Begriffe. Gemeinhin wird darunter eine Berechtigung an den Daten bzw. die Verantwortlichkeit für die Datenbearbeitung verstanden.

Das Dateneigentum ist vornehmlich Gegenstand akademischer Diskussion. Der Bundesrat hat in der Botschaft zum VE-DSG die Schaffung einer solchen Rechtsfigur, auch mit Verweis auf die Rechtsentwicklung in der EU, abgelehnt.

Die Datenhoheit umschreibt eher eine faktische Verfügungsmacht über die Daten. Im Allgemeinen wird dem Einzelnen eine Datenhoheit an seinen eigenen Daten zugeschrieben. Er hat einen grundrechtlichen Anspruch auf den Schutz der Privatsphäre (Art. 13. Abs. 2 Bundesverfassung) und kann sich gegen eine unrechtmässige Datenbearbeitung sowohl zivilrechtlich wehren also auch ihre Rechte gestützt auf das Datenschutzgesetz geltend machen (Berichtigung, Sperrung, Löschung). In diesem Sinne steht ihm die Datenhoheit zu, d.h. er kann über verschiedene Optionen – so diese zur Verfügung stehen – über die Bearbeitung und Nutzung «seiner» Daten selbst bestimmen.

Das Datenschutzrecht spricht seinerseits vom Verantwortlichen, wenn es das Unternehmen oder den Staat meint. Die Verantwortlichkeit heisst hier, dass sichergestellt werden muss, dass die Datenbearbeitung rechtlich korrekt ist, mit allem was das heisst. Verantwortlich ist derjenige, der – auf Basis einer gültigen Rechtsgrundlage – festlegen kann, welche Daten für welchen Zweck gesammelt werden.

5. Datenkategorien ITS-Richtlinie

Wenn wir von Mobilitätsdaten im Rahmen der intelligenten Mobilität und der multimodalen Mobilität sprechen, finden sich die benötigten Datenkategorien in der Rechtssetzung der EU, insbesondere in der ITS-Richtlinie und den darauf basierenden delegierten Verordnungen. Die delegierten Verordnungen benennen Kategorien von Daten, die bereitgestellt werden sollen, um Verkehrsströme sicherer, effizienter und nachhaltiger, sprich intelligenter, zu machen. Es werden nur die «Resultate» vorgegeben, also welche Daten vorhanden sein sollen, aber nicht wie man zu diesen Daten kommt. Folgende Kategorien werden dabei in den Verordnungen definiert[4]:

5.1 Delegierte Verordnung (EU) 2015/962 – Echtzeit-Verkehrsinformationsdienste (RTTI)

Die Verordnung legt die Spezifikationen fest, die nötig sind um die Bearbeitung und den Austausch von Daten für Echtzeit-Verkehrsinformationsdienste zu ermöglichen. Sie definiert dazu die gewünschten Daten innerhalb von drei Kategorien, die im Anhang weiter definiert werden:

- Statische Strassendaten
- Dynamische Stassenstatusdaten
- Verkehrsdaten

[4] Die nachfolgenden Ausführungen beruhen auf dem Stand der Verordnungen im November 2020. Verschiedene delegierte Rechtsakte wie auch die Richtlinie selber werden momentan oder in naher Zukunft revidiert. Weitere Datenkategorien können dabei definiert werden.

5.2 Delegierte Verordnung (EU) 886/2013 – Verkehrsinformationen Strassenverkehrssicherheit (SRTI)

Als sicherheitsrelevante Ereignisse und Bedingungen werden die folgenden Kategorien definiert:

a) Vorübergehend rutschige Fahrbahn
b) Tiere, Personen, Hindernisse, Gegenstände auf der Fahrbahn
c) Ungesicherte Unfallstellen
d) Kurzzeitbaustellen
e) Eingeschränkte Sicht
f) Falschfahrer
g) Nicht ausgeschilderte Strassenblockierungen
h) Aussergewöhnliche Witterungsbedingungen

5.3 Delegierte Verordnung (EU) 2017/1926 – multimodale Reiseinformationsdienste (MMTI)

Im Bereich der multimodalen Reiseinformationsdienste sollen zum einen statische Reise- und Verkehrsdaten und historische Verkehrsdaten (gemäss Anhang 1 zur Verordnung), zum andern dynamische Reise und Verkehrsdaten verschiedener Verkehrsträger zur Verfügung gestellt werden (Anhang 2). Dabei geht es insbesondere um die Ermöglichung der Standortsuche, der Routenberechnung und der Vorhersage von Fahrzeiten.

5.4 Delegierte Verordnung (EU) 885/2013 – Parkplätze für LKW

Ziel dieser Verordnung ist es, durch die Einführung von Informationsdiensten die Nutzung von Parkplätzen für LKW zu optimieren und den Fahrern bzw. den Beförderungsunternehmen die Entscheidung über Zeitpunkt und Ort des Parkens zu erleichtern.

Zu erheben sind statische Parkplatzdaten (Name und Adresse des LKW-PP, Ortsangabe, Kennung der Strasse, Angabe der Ausfahrt, Gesamtzahl der Stellplätze, Preis und Währung), Informationen über Sicherheit und Ausrüstung, Kontaktangaben des Parkplatzbetreibers und dynamische Daten über freie Stellplätze (Verfügbarkeit, Belegung).

5.5 Delegierte Verordnung (EU) 305/2013 eCall

Die eCall-Initiative – ein automatisches Notrufsystem für Fahrzeuge – nimmt eine spezielle Stellung unter den auf der ITS Richtlinie basierenden delegierten Verordnungen ein. Bereits bei Erlass der delegierten Verordnung 2012 bestand eine gewisse Klarheit in Bezug auf das einzuführende System und es bestanden bereits europäische Normen zur technischen Umsetzung. Zudem war klar, dass im System Personendaten bearbeitet werden würden und die delegierte Verordnung legte bereits fest, wer für die Datenbearbeitung verantwortlich sein soll, nämlich die Notrufabfragestellen und deren Dienstleistungspartner (Art. 6).

Im Nachgang zur delegierten Verordnung wurden weitere Rechtsinstrumente zur Einführung des eCall erlassen, unter anderem auch eine separate Durchführungsverordnung zu den datenschutzrechtlichen Rahmenbedingungen (Durchführungsverordnung (EU) 2017/78). Darin wird – abgestützt auf Empfehlungen der Artikel-29-Datenschutzgruppe von 2006[5] – festgelegt, dass das eCall System nicht verfolgbar und nicht von aussen zugänglich sein darf, und dass Daten im internen Speicher automatisch und fortlaufend gelöscht werden müssen. Dem Hersteller des Systems wurde zudem eine Informationspflicht gegenüber dem Fahrzeughalter auferlegt (inklusive Musterformular), und er muss die Informationssicherheit gewährleisten.

Im Gegensatz dazu bestehen bei den übrigen delegierten Verordnung momentan noch mehr Lücken, wie die Umsetzung technisch gestaltet werden soll und wer welche Verantwortung trägt. Dies soll im

[5] Arbeitsdokument: Eingriffe in den Datenschutz im Rahmen der Initiative eCall, 01609/06/DE WP 125

Folgenden beispielhaft an den Datenkategorien der Verordnung hinsichtlich der Bereitstellung von Echtzeit-Informationsdiensten aufgezeigt werden.

6. Datenschutzrechtliche Bewertung Mobilitätsdaten

6.1 Datenschutzrechtliche Normen in den Rechtsgrundlagen

Die *ITS Richtlinie* enthält in Art. 10 Vorgaben zum Datenschutz und verweist auf die entsprechenden EU-Normen (Richtlinie 95/46/EG, heute ersetzt durch die DSGVO). Zusätzlich werden generelle Vorgaben zur Informationssicherheit, zur Datenminimierung, zur Verhältnismässigkeit und zur Einwilligung gemacht. Die *delegierten Verordnungen* verweisen jeweils in den Erläuterungen auf die Wichtigkeit des Datenschutzes und postulieren klar, dass bei der Einführung und Nutzung intelligenter Verkehrssysteme Personendaten bearbeitet werden, ohne diese jedoch zu spezifizieren. Spezifischere Normen enthalten die delegierten Verordnungen jedoch nicht.

6.2 Personendaten oder Sachdaten?

Am Beispiel der delegierten Verordnung zu den Echtzeit-Informationsdiensten (RTTI) soll exemplarisch aufgezeigt werden, welche Überlegungen in Bezug auf den Datenschutz relevant sind.

Die Verordnung enthält im Anhang die verschiedenen Datenkategorien, die von den Strassenverkehrsbehörden und Strassenbetreibern zur Verfügung gestellt werden müssen. In den statischen Strassendaten sind das unter anderem Angaben zu den physischen Merkmalen des Strassennetzes oder zu Verkehrszeichen. Dynamische Strassenstatusdaten liefern beispielsweise Informationen zu Sperrungen, Baustellen oder Unfällen. Und schliesslich die Verkehrsdaten, die Angaben zum Verkehrsaufkommen, zu Staus oder Reisezeiten machen sollen. Datenschutzrechtlich muss als erstes geklärt werden, ob es sich bei diesen Informationen überhaupt um Personendaten handelt. Nur dann kommen die strengen Regeln des Datenschutzrechts zur Anwendung.

Auf den ersten Blick erscheint klar, dass in der Information selber keine Personendaten enthalten sind. Angaben zur Strassenbreite oder dem Standort einer Ladestation für Elektrofahrzeuge sind reine Sachdaten. Bei genauerem Hinsehen stellt sich jedoch die Frage, wie diese Daten überhaupt entstehen können, und ob bei der Erstellung der Information Personendaten benötigt werden oder auch unbeabsichtigt anfallen.

Die Verordnung macht keine Aussagen dazu, wie die benötigten Informationen entstehen. Es ist wahrscheinlich, dass zumindest für gewisse unter ihnen die Erhebung von Personendaten irgendwo im Prozess vorkommt. Klarerweise ist dies der Fall bei der Kategorie «Verkehrsdaten»: An und für sich stecken in Angaben zum Verkehrsaufkommen oder zur Länge des Verkehrsstaus keine Personendaten. Wenn aber davon ausgegangen wird, dass diese Angaben zustande kommen aus Daten, die in einzelnen Fahrzeugen entstehen und von Fahrzeug zu Fahrzeug oder vom Fahrzeug an eine Infrastruktur weitergegeben werden, handelt es sich um Personendaten. Dies entspricht dem heutigen Stand der Diskussion und wurde von verschiedenen damit befassten Organen der EU so interpretiert (siehe dazu unten «Exkurs Datenbearbeitung C-ITS»). In wie weit und bei welchen Bearbeitern die Personendaten anfallen, ist dann wiederum eine Frage der technischen Umsetzung (Verschlüsselung oder frühe Anonymisierung können den Kreis der Bearbeiter klein halten).

Aber auch bei anderen Informationen zum Verkehrsgeschehen ist vorstellbar, dass Personendaten irgendwo im Zyklus bearbeitet werden, ohne dass diese direkt aus dem Fahrzeug stammen. Als Beispiel mag ein Unfall dienen, bei dem eine Meldung an die Polizei und die Sanität geht. Beide werden im Rahmen ihrer Tätigkeit Personendaten bearbeiten und sei es nur via das Nummernschild eines beteiligten Fahrzeugs. Anschliessend kommt es darauf an, wie aus dieser Information eine Unfallmeldung an die Öffentlichkeit erarbeitet wird und wie sichergestellt wird, dass allfällige Informationen zu einer Person nicht Teil dieser Meldung sind. Idealerweise wird der Personenbezug der Information so früh als möglich entfernt und die Daten werden anonymisiert. Jede weitere Bearbeitung bezieht sich dann nur noch auf Sachdaten.

Damit wird klar, dass sich die verschiedenen Datenkategorien der delegierten Verordnungen der ITS Richtlinie oder auch Abgrenzungen wie sie im Entwurf mmM zum Kerndatenset des BAV vorgenommen werden[6], nicht im gleichen Mass für eine datenschutzrechtliche Abgrenzung eignen. Nachfolgend deshalb der Versuch, die Abgrenzung von Personen- und Sachdaten an bestimmten Prozesspunkten festzumachen.

Standorte von fixen Objekten, zum Beispiel eine Haltestelle oder ein Parkplatz, sind datenschutzrechtlich wenig problematisch. Standorte von beweglichen Objekten, zum Beispiel das Fahrrad eines Sharinganbieters, müssen aber genauer angeschaut werden. Hier muss die Frage gestellt werden, woher die Information zum jeweiligen Standort kommt. Wenn dieser personenbezogen hergeleitet wird, z.B. hat eine für den Anbieter identifizierte Person das Fahrrad an einem bestimmten Ort abgestellt, muss im Prozess sichergestellt werden, dass die Information zur betroffenen Person nur dort vorhanden ist, wo sie vorhanden sein darf und dass anschliessend eine Anonymisierung oder Aggregation vorgesehen ist, bevor die Information an andere Verkehrsteilnehmende weitergegeben wird.

Analog bei *Angaben zum Betrieb*, zu spezifischen Situationen oder zu Strassenverhältnissen: stammen die Angaben zu diesen Situationen aus einer «neutralen» Quelle, zum Beispiel dem Wetterbericht oder es handelt sich um eine Angabe zu verfügbaren Parkflächen oder Fahrrädern gemäss einem Plan, ist das eher unproblematisch. Stammt die Information zu einer Parkfläche aber aus einer Videoüberwachung vor Ort oder der Strassenzustand wird über die Sensoren von Fahrzeugen weitergeben, handelt es sich unter Umständen um Personendaten, die – analog zu oben – nur dort genutzt werden dürfen, wo dies zulässig ist.

Eine weitere Unterscheidung kann gemacht werden zwischen der reinen *Bereitstellung von Informationen*, also dem Standort eines Angebots, dem Netz für eine Route, dem Preis für eine Leistung oder der Ausstattung eines Fahrzeugs, und der *Abfrage* dieser Information. Wenn die Nutzerin, um vom Standort eines Angebots profitieren zu können, ihren eigenen Standort angeben muss, muss sie sich diesbezüglich identifizieren und ihre Personendaten werden bearbeitet. Analog wenn der Nutzer eine Abfrage macht, ob eine bestimmtes Fahrzeug behindertengerecht ausgestaltet ist. Im Moment der Abfrage gibt der Nutzer unter Umständen seine Gesundheitsdaten bekannt – seine Behinderung – deren Bearbeitung nur unter den Voraussetzungen des Datenschutzrechts zulässig ist. Und natürlich auch im Moment, wo eine Leistung reserviert oder bezahlt werden soll. Hier muss sich die Nutzerin gegenüber dem Anbieter identifizieren und diese Information darf nur mit denjenigen geteilt werden, die eine entsprechende Berechtigung haben.

Nun heisst aber das (potentielle) Vorliegen von Personendaten nicht, dass eine Datenbearbeitung nicht möglich ist. Eine Umsetzung ist jeweils in verschiedenen technischen Varianten möglich, die mehr oder weniger datenschutzkonform sein können. Aus dem Grundsatz der Datenminimierung ergibt sich, dass so wenig Personendaten wie nötig bearbeitet werden sollen. Werden Personendaten bearbeitet, so gelten die Vorgaben des jeweiligen Datenschutzrechts und die oben ausgeführten Prinzipien kommen zur Anwendung. Die Datenbearbeitung muss recht- und verhältnismässig sein und die Rechte der Betroffenen geschützt. Idealerweise werden jeweils Systeme entwickelt, die ohne Personendaten funktionieren, beispielsweise die Angabe verfügbarer Parkplätze nicht über eine Kamera, sondern mittels Sensoren in der Parkfläche. Wichtig ist deshalb der Einbezug des Datenschutzes bereits in die Entwicklung der Umsetzungsprojekte. Nur dort kann im konkreten Fall definiert werden, ob es sich um Personendaten handelt, ob ein Rechtfertigungsgrund vorliegt und wie die datenschutzkonforme Nutzung der Daten sichergestellt wird.

Exkurs – Datenbearbeitung C-ITS

Es gibt verschiedene Gremien auf Stufe EU und international, die sich mit der datenschutzrechtlichen Einordnung von Datenbearbeitungen beim automatisierten und vernetzten Fahren beschäftigt haben.

[6] Netzdaten, Betriebsdaten, Fahrzeugdaten, Vertriebsdaten, Informationsdaten (NaDIM: Nationale Dateninfrastruktur Mobilität, Gesetzesvorlage in Bearbeitung)

Die **C-ITS Plattform** hat sich insbesondere mit der datenschutzrechtlichen Einschätzung der CAM (cooperative awareness messages) und DENM (decentralised environmental notification messages) auseinandergesetzt. Dabei handelt es sich um die Basis der Kommunikation beim vernetzten Fahren, wenn Maschinen mit Maschinen kommunizieren, seien das Fahrzeuge oder Infrastrukturelemente. Die Grundidee besteht darin, dass Fahrzeuge ihr Umfeld direkt und «selber» über sich und ihr Verhalten informieren und solche Informationen von anderen Fahrzeugen oder der Infrastruktur erhalten. Die Standards wurden von europäischen Standardisierungsorganisationen (ETSI, CEN) entwickelt und bilden die Basis des Informationsaustauschs im vernetzten Verkehr.

Die Arbeitsgruppe zum Datenschutz der C-ITS Plattform («Working Group on Data Protection and Privacy») hat die nötigen datenschutzrechtliche Abklärungen vorgenommen, die dann Eingang in den Schlussbericht der C-ITS Plattform gefunden haben. Dort wird festgehalten, dass die in CAM und DENM ausgetauschten Informationen als Personendaten gelten, da die Nutzenden (indirekt) identifizierbar sind.[7]

Diese Einschätzung wurde der **Artikel-29-Datenschutzgruppe** zur Stellungnahme vorgelegt. Bei dieser handelte es sich um die unabhängige europäische Arbeitsgruppe, die sich bis zum Inkrafttreten der DSGVO 2018 mit der Auslegung der Richtlinie 95/46/EC beschäftigte. Sie wurde mit Inkrafttreten der DSGVO durch den **Europäischen Datenschutzausschuss, EDSA** ersetzt. Die angefragte Artikel-29-Datenschutzgruppe stellt zuerst klar, dass ihre Stellungnahme nur für sogenannte «day-one applications» gelte, bei denen es sich vor allem um Funktionalitäten zum Strassenzustand handelt, ohne dass die Fahrerin die Kontrolle über das Fahrzeug abgibt; höhere Vernetzungsstufen müssen dem EDSA erneut vorgelegt werden. Die Artikel-29-Datenschutzgruppe bestätigte, dass es sich bei CAM und DENM – für den Bearbeiter – um (pseudonymisierte) Personendaten handelt. Es wurde argumentiert, dass zum einen die zu benutzenden Zertifikate mit dem Absender, also dem Fahrzeug verbunden sind, und zum andern, dass insbesondere CAM Lokalisierungsangaben enthalten, die relativ einfach zu einer Identifizierung führen können. Die Artikel-29-Datenschutzgruppe hat anschliessend die Rechtmässigkeit einer derartigen Datenbearbeitung geprüft und kam zum Schluss, dass längerfristig eine gesetzliche Grundlage (im Unionsrecht) erarbeitet werden muss, um eine genügende Basis für die Datenbearbeitung zu schaffen. Da es sich bei C-ITS um eine Anwendung handelt die Verkehrssicherheit, Effizienz und Nachhaltigkeit sichern soll, könne die Grundlage nicht alleine in der Einwilligung oder in der vertraglichen Vereinbarung zwischen Anbieterin und Nutzer liegen. Zusätzlich wurde empfohlen das legislative Projekt mittels einer Datenschutzfolgenabschätzung zu begleiten.

Der **EDSA** hat seinerseits im Januar 2020 eine Leitlinie zum automatisierten Fahrzeug veröffentlicht. Das Papier grenzt sich zu Fragen von C-ITS ab, mit der Begründung, dass die datenschutzrechtlichen Fragen bei der Kommunikation zwischen Fahrzeugen bzw. zwischen Fahrzeugen und der Infrastruktur sehr spezifisch und noch nicht ausdiskutiert seien. Die in der Leitlinie behandelten Fallstudien fokussieren mehrheitlich auf die Datenbearbeitung im Fahrzeug und deren Austausch mit Anbietern von Dienstleistungen (z.B. Versicherung, Parkplatzbuchung, Unfallstudien, Informationen im Mietfahrzeug, aber auch eCall, obwohl es sich hier schon eher um C-ITS Anwendung handelt). Für die Rechtmässigkeit der jeweiligen Datenbearbeitung stellt der Ausschuss eher auf die Einwilligung oder eine vertragliche Abmachung zwischen Datenlieferant und Datenempfänger. Es wird aber auch an die hohen Anforderungen an eine derartige Einwilligung erinnert, die sowohl die Halterin wie auch den Fahrer betreffen kann und auch jederzeit wieder zurückgezogen werden kann.

Die **Internationale Konferenz der Datenschutzbehörden** hat 2017 eine Resolution zum Datenschutz beim automatisierten Fahren verabschiedet und darin unter anderem gefordert, dass die Persönlichkeitsrechte der Betroffenen geschützt werden, insbesondere durch transparente Information, vor allem auch bei der Verwendung von selbstlernenden Algorithmen, Anonymisierung von Personendaten wo immer möglich, kurze Aufbewahrungsfristen, schnelle Löschung von Daten, die nicht mehr benötigt werden, Kontrollmechanismen für Betroffene zur Verfügung stellen, Datensicherheit gewährleisten etc.

[7] "*After an in-depth analysis, WG4 concluded that those messages are considered as "personal data" because of the potential of indirect identification of users. The European legislation on Data Protection 95/46/EC is therefore considered applicable (…).*", C-ITS Platform, Final report, January 2016, S. 48

Als Erweiterung des Rahmens für das automatisierte Fahren sei auch auf datenschutzrechtliche Anforderungen an **Systeme künstlicher Intelligenz** generell verwiesen. Je höher der Automatisierungsgrad umso fortgeschrittener wird der zugrundeliegende Algorithmus sein. Aus datenschutzrechtlicher Sicht stellen sich nochmals ganz andere Anforderungen an die Entwicklung und Nutzung solcher Systeme, zum Beispiel im Hinblick auf die Trainingsdaten, die Testdaten, die Nachvollziehbarkeit der Resultate (Stichwort «automatisierte Einzelentscheidung»), die Rückkoppelung von Ergebnissen oder die Selbstveränderung des Systems. Eine detaillierte Analyse würde im vorliegenden Papier zu weit führen. Die noch ausstehende Analyse im Rahmen des Projekts «Ethik und automatisiertes Fahren» wird dazu nützliche Elemente liefern.

6.3 Spezifische Risiken Mobilitätssektor

Nicht jede Bearbeitung von Personendaten setzt die Betroffenen dem gleichen Risiko aus. Das zentrale datenschutzrechtliche Risiko im Mobilitätssektor besteht in der umfangreichen digitalen Erfassung der alltäglichen Wege, Aktivitäten und Kontakte der gesamten Bevölkerung. Potentiell handelt es sich hier um eine Datenbearbeitung mit grosser Breitenwirkung.

Bezüglich der Datenkategorien sind vor allem drei Bereiche besonders anfällig für Persönlichkeitsverletzungen.

a) *Geolokalisierungsdaten*: da hier die Identifikation der einzelnen Person relativ einfach ist und – in Kombination mit einer Zeitangabe – die Daten zu einem Persönlichkeitsprofil verdichtet werden können.
b) *Biometrische Daten*: zum Beispiel der Fingerabdruck oder die Gesichtserkennung für den Zugang zu Fahrzeugen oder zur Identifizierung von Nutzenden. Das besonders schützenswerte an biometrischen Daten liegt in ihrer Unveränderlichkeit und dem untrennbaren Bezug zur Person. Ein Passwort kann geändert werden, der Fingerabdruck bleibt. Wer im Besitz dieser Daten ist, hat ein grosses Potential einer Person nachhaltig zu schaden.
c) *Daten, die strafrechtlich relevant sein können*, werden im Datenschutzrecht als besonders schützenswert betrachtet, da hier das Stigmatisierungspotential hoch ist. Im Bereich des Verkehrs kann es hier um Angaben zu Verkehrsregelverletzungen oder zu einem Unfallhergang gehen.

Wie bereits oben ausgeführt, heisst dies nicht, dass derartige Daten nicht bearbeitet werden dürfen. Abgesehen vom adäquaten Rechtfertigungsgrund und der Verhältnismässigkeit der Bearbeitung, müssen hier verstärkte Schutzmassnahmen zum Zug kommen, zum Beispiel:

- Nur bearbeiten, wenn für Zweck unbedingt nötig und nur lokal bearbeiten, keine Zentralisierung
- Kurze Aufbewahrungsfristen
- Verschlüsselung der Daten und schnelle Pseudonymisierung und Anonymisierung
- Zugang zu den Daten restriktiv handhaben
- Erhöhte Transparenz (welche Daten, wann, warum, wo gespeichert)
- Deaktivierung des Dienstes ermöglichen, der die Daten braucht und Alternativen offerieren
- Keine Rohdaten für biometrische Authentifikation speichern, auch nicht lokal
- Strafrechtlich relevante Daten nicht von Privaten bearbeiten lassen

Sowohl der EDSA wie auch seine Vorgängerin, die Artikel-29-Datentschutzgruppe, weisen in ihren oben erwähnten Ausführungen zudem auf die spezifischen datenschutzrechtlichen Risiken beim automatisierten und vernetzen Fahren hin. Dazu gehören:

- C-ITS macht neu Informationen zugänglich, die bis jetzt privat waren, nämlich wohin wir wie fahren. Diese Information wird mit andern Verkehrsteilnehmenden geteilt und erlaubt eine Art «verteilte permanente Verhaltensüberwachung» von allen durch alle.
- Die Informationsasymmetrie und der damit verbundene Mangel an Kontrolle über die Daten durch die Fahrerin, den Passagier oder die Halterin, aber auch zwischen Sender und Empfängerin: statt einer eins-zu-eins-Kommunikation werden die Nachrichten an eine unbekannte Anzahl Personen bzw. Fahrzeuge übermittelt.

- Es herrscht momentan noch ein Mangel an Transparenz – was wird übertragen? An wen? Was machen die damit? Wer ist wofür verantwortlich?
- Mangelnde Transparenz besteht auch für Fahrzeugführer und Fahrgäste. Eventuell wird nur der Halter über die Bearbeitung und Verwendung der Daten informiert, der aber nicht Fahrzeugführer ist. Sensoren überwachen auch das Fahrzeugumfeld, dort können Personen erfasst werden, die über die Datenbearbeitung nicht informiert sind.
- Das Interesse an den Daten ist vielfältig, sowohl von staatlicher Seite (Durchsetzung Verkehrsregeln) wie von Privater (kommerzielle Interessen). Dadurch besteht die Gefahr des «function creep», das heisst, die Personendaten werden für einen bestimmten Zweck gesammelt, finden dann aber andere, weitere Anwendungsmöglichkeiten, die von der ursprünglichen Zweckbestimmung nicht gedeckt sind.
- Zudem besteht die Gefahr, dass übermässig Daten gesammelt werden durch die zahlreichen Sensoren in Fahrzeugen.

6.4 Verantwortlichkeit Mobilitätssektor

Verantwortlich für die Einschätzung der oben aufgezählten Risiken und die Umsetzung geeigneter Massnahmen ist rechtlich gesehen der für die Bearbeitung Verantwortliche. Also derjenige, der Zweck und Mittel bestimmt. Gerade im Mobilitätssektor ist die Festlegung des Verantwortlichen für die Datenbearbeitung nicht ganz einfach. Digitale Mobilitätsdienste sind geprägt von einer Vielzahl von Beteiligten, die in komplexen Strukturen zusammenarbeiten. Da kann der Staat als Plattformanbieter fungieren, die Entwicklerin eine App gestalten, der Betreiber die App anbieten, die Dienstleisterin den der App zugrundeliegenden Service anbieten, der Nutzer den Service und die App nutzen etc. Insoweit die verschiedenen Beteiligten Personendaten bearbeiten, muss ihre jeweilige Verantwortlichkeit anhand der konkreten Prozesse geklärt werden.

Beim automatisierten und vernetzen Fahrzeug kann der Verantwortliche ein Dienstleistungsanbieter sein oder der Fahrzeughersteller. Er bestimmt Zweck und Mittel der Bearbeitung. Demgegenüber kann der Fahrzeughalter oder eine Fahrzeugführerin kaum als verantwortlich für die Datenbearbeitung gesehen werden: wenn davon ausgegangen wird, dass der Verantwortliche derjenige ist, der die Datenbearbeitung «anbietet», den Nutzen daraus zieht und auch eine tatsächliche Einflussmöglichkeit auf die Art und den Umfang der Datenbearbeitung hat, dann kommen Halter und Fahrerin eher nicht in Frage für diese Rolle. Sie sind als von der Bearbeitung betroffene Personen zu betrachten.

7. Datenschutzfolgenabschätzung (DSFA)

Das Instrument der Datenschutzfolgenabschätzung wurde mit der DSGVO europaweit eingeführt. Eine DSFA enthält eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und spezifiziert im Ergebnis technische und organisatorische Massnahmen zur Bewältigung der erwarteten Datenschutz-Risiken. Nach Art. 35 DSGVO muss eine DSFA durchgeführt werden, wenn die Datenbearbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt.

Der VE-DSG sieht neu in Art. 22 die DSFA ebenfalls vor. Sie gilt als Instrument, um Risiken zu erkennen und zu bewerten, die für die betroffene Person durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Auf der Basis dieser Abschätzung sollen gegebenenfalls angemessene Massnahmen definiert werden, um diese Risiken für die betroffene Person zu bewältigen.

Nach Art. 22 Abs. 3 VE-DSG muss in der DSFA zunächst die geplante Bearbeitung dargelegt werden. So müssen beispielsweise die verschiedenen Bearbeitungsvorgänge (z. B. die verwendete Technologie), der Zweck der Bearbeitung oder die Aufbewahrungsdauer aufgeführt werden. Im Weiteren muss gemäss Absatz 3 aufgezeigt werden, welche Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person die fraglichen Bearbeitungsvorgänge mit sich bringen können. So ist darzustellen, in welcher Hinsicht von der fraglichen Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person ausgeht und wie dieses Risiko zu bewerten ist. Schliesslich muss die DSFA erläutern, mit welchen Massnahmen diese Risiken bewältigt werden sollen. Massgebend

dafür sind insbesondere die Grundsätze nach Artikel 5 VE-DSG, aber auch die Pflicht zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen (privacy by design/by default; Art. 6 VE-DSG). Bei diesen Massnahmen kommt es auch zu einer Abwägung zwischen den Interessen der betroffenen Person und denjenigen des Verantwortlichen. Diese Interessenabwägung ist in der DSFA ebenfalls aufzuführen und entsprechend zu begründen. Massnahmen zur Gewährleistung der Informationssicherheit können sowohl technische als auch organisatorische sein. So zum Beispiel mit Berechtigungskonzepten für die Gewährleistung der Vertraulichkeit, Massnahmen zur sicheren Authentifizierung, Festlegung der Kommunikationskanäle, Gebäudesicherheit, Festlegung organisatorischer Abläufe und vertragliche Verpflichtungen, Verschlüsselung etc.

In der Botschaft des Bundesrates heisst es für die Bundesorgane: «Das Vorgehen gemäss der Projektmanagementmethode Hermes dürfte den Anforderungen einer Datenschutz-Folgenabschätzung weitgehend entsprechen.»[8] (S. 7059)

8. Schlussfolgerung und weitere Schritte

Die vorangegangenen Ausführungen haben gezeigt, dass die datenschutzrechtlichen Fragestellungen im Bereich der Mobilität ein weites Feld sind. Viele Fragen sind noch offen, auch weil die Umsetzung in weiten Bereichen noch in der Zukunft liegt und heute nur begrenzt abgeschätzt werden kann. Zudem versucht das vorliegende Papier den Bogen vom multimodalen Reiseplaner bis hin zum selbstfahrenden Auto zu schlagen, auch wenn die datenschutzrechtliche Problematik nicht durchweg vergleichbar ist. Nichtsdestotrotz bestehen gewisse Gemeinsamkeiten unabhängig vom Modell, das angeschaut wird. So zählen Lokalisierungs- und Bewegungsdaten von Menschen sicher zu den heikleren Gebieten, auf denen sich der Staat bewegen will. Daneben gibt es aber auch ein weites Feld von reinen Sachdaten, deren Nutzung weniger Hindernisse im Weg stehen.

Es ist zentral, dass datenschutzrechtliche Konformität von Anwendungen als Voraussetzung für jede Umsetzung gesehen wird. Die konsequente Anwendung der datenschutzrechtlichen Regelungen hilft die persönliche Autonomie der Menschen im Umgang mit Maschinen zu schützen. Dies wiederum schafft Vertrauen in Anwendungen und damit auch den Boden für allfällige Anwendungen.

Das bedingt, dass der Datenschutz von Anfang an und bis zum Schluss in die Entwicklung von Anwendungen einbezogen ist. Gerade bei konkreten Projekten ist der begleitende Austausch unerlässlich. Der Datenschutz ist kein absolutes Recht; er muss in einer Güterabwägung mit anderen Anforderungen, wie zum Beispiel der Sicherheit oder der Nutzerfreundlichkeit, immer wieder auf den Prüfstand gestellt werden. Der Datenschutz basiert auf Prinzipien und gibt (leider) keinen einfachen und klaren Regelsatz vor, der sicherstellt, dass eine Anwendung datenschutzkonform ist.

Das Papier zeigt auch klar, dass Überlegungen zum Datenschutz nur im interdisziplinären Austausch fruchtbar sind. Bereits der Entscheid, ob es sich bei gewissen Daten um Personendaten handelt oder nicht, kann nur getroffen werden, wenn klar ist, von welchen Daten wir reden. Ebenso müssen allfällige Sicherheitsmassnahmen oder Massnahmen zur Pseudonymisierung oder Anonymisierung von Daten gemeinsam entwickelt werden.

Auf der Basis der vorliegenden Ausführungen wird vorgeschlagen folgende Schritte anzugehen bzw. weiterzuverfolgen:

- **Verkehrsdatenplattform** ASTRA: Basierend auf dem heutigen Piloten sollten weitere Datenkategorien für die Bearbeitung in der VDP erarbeitet und datenschutzrechtlich analysiert werden.

- Projekt **Stauendewarnung**: Eine datenschutzrechtliche Begleitung des Projekts sollte vorgesehen werden.

[8] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 7059

- **Datenbearbeitung im** (automatisierten) **Fahrzeug**: Im Rahmen der laufenden Revision der Verordnung über die technischen Anforderungen an Strassenfahrzeuge (VTS, SR 741.41) wurde ersichtlich, dass der Bearbeitung von Personendaten in Fahrzeugen bereits heute höhere Beachtung geschenkt werden soll. Eine Analyse der gängigen Bearbeitungsformen im Fahrzeug soll abgeglichen werden mit den Bedürfnissen des ASTRA im Hinblick auf die Vernetzung von Fahrzeugen und Infrastruktur sowie die Schaffung einer offenen fahrzeuginternen Plattform.

- **Vernetzung Verkehr**: die (datenschutzrechtlichen) Entwicklungen in Bezug auf vernetzte Verkehrssysteme soll weiter beobachtet werden. Beispiele nationaler Umsetzungen der ITS-Richtlinie in europäischen Ländern, insbesondere Finnland, Österreich, Niederlande, sollen studiert und als mögliche Basis für zukünftige Gesetzgebung in der Schweiz herangezogen werden.

- **Pseudonymisierung / Anonymisierung**: Vertiefte Abklärungen betreffend der datenschutzrechtlichen Konformität des pseudonymisierten Austauschs von Daten im vernetzten Verkehr sind vorzunehmen.

- **Nationale Dateninfrastruktur** (NaDIM): Das Einbringen datenschutzrechtlicher Anliegen, mit einem besonderen Fokus auf die Bedürfnisse des ASTRA, soll weitergeführt werden (= Massnahmen MD5 und MV7 von mmM, die das ASTRA verantwortet).

- **Vertrauenswürdige Datenräume** sind auf europäischer Ebene wie auch in der Bundesverwaltung ein wichtiges Thema. Sie können unter Umständen Bedingungen schaffen, die die Bearbeitung von personenbezogenen Daten, gerade aus dem Mobilitätsbereich, vereinfachen können. Deshalb ist das Einbringen der Mobilitätsbedürfnisse (des ASTRA) an der Initiative «Digitale Selbstbestimmung» und der Schaffung vertrauenswürdiger Datenräume notwendig. Das Thema Mobilität bietet sich exemplarisch als Modell für die Schaffung eines derartigen Datenraumes an.

9. Gesetze / Materialien

9.1 Gesetzgebung Schweiz

- Bundesverfassung vom 18. April 1999 (BV), SR 101
- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1
- Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz, 235.11
- Entwurf, Bundesgesetz über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 7193), https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf
- Revidiertes DSG, Text gemäss Schlussabstimmung, https://datenrecht.ch/ndsg-ohne-botschaft/
- Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 6941), https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf
- Bundesgesetz vom 28. September 2018 über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG), SR 235.3
- Strassenverkehrsgesetz vom 19. Dezember 1958 (SVG), SR 741.01
- Verordnung vom 19. Juni 1995 über die technischen Anforderungen an Strassenfahrzeuge (VTS), SR 741.41
- Strategie digitale Schweiz vom 11. September 2020, https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz.html

9.2 Datenschutz Europa

- Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung, DSGVO**), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=de
- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (*ausser Kraft*), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=DE
- Richtlinie (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L0680&from=DE
- Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (*ausser Kraft*), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32008F0977&from=DE
- Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Europarat Konvention **SEV 108**, https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108

9.3 ITS Europa

- Richtlinie 2010/40/EU vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (**ITS Richtlinie**), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010L0040

- Delegierte Verordnung (EU) 2015/962 vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32015R0962&from=EN
- Delegierte Verordnung (EU) 886/2013 vom 15. Mai 2013 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf Daten und Verfahren für die möglichst unentgeltliche Bereitstellung eines Mindestniveaus allgemeiner für die Strassenverkehrssicherheit relevanter Verkehrsinformationen für die Nutzer, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0886&from=EN
- Delegierte Verordnung (EU) 2017/1926 vom 31. Mai 2017zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter multimodaler Reiseinformationsdienste (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32017R1926&from=EN)
- Delegierte Verordnung (EU) 305/2013 vom 26. November 2012 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0305&from=EN
- Delegierte Verordnung (EU) 885/2013 vom 15. Mai 2013 zur Ergänzung der IVS-Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die Bereitstellung von Informationsdiensten für sichere Parkplätze für Lastkraftwagen und andere gewerbliche Fahrzeuge,https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0885&from=EN

9.4 ITS und Datenschutz Europa

- C-ITS Platform Final Report with Annexes, Phase I, January 2016, https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf
- C-ITS Platform Final Report with Annexes, Phase II, September 2017, https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf
- Artikel-29-Datenschutzgruppe, Stellungnahme 03/2017 zur Verarbeitung personenbezogener Daten im Kontext Kooperativer, Intelligenter Verkehrssysteme (C-ITS), WP 252, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171
- Europäischer Datenschutz-Ausschuss (EDSA), Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_de
- 39. Internationale Konferenz der Datenschutzbehörden, Resolution on Data Protection in Automated and Connected Vehicles, https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf