Rechtsfragen bei Geoportalen

am Beispiel der Leitungsnetzauskunft des Zweckverbands Grevesmühlen

Prof. Dr. Alexander Roßnagel /
Dipl.-Betriebsw. (FH) Dennis Hoss, LL.M.

Dezember 2010

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

Inhalt

1 Fragestellung ... 1

2 Grundlagen ... 2
2.1 Rechtsstellung des Zweckverbands Grevesmühlen ... 2
2.2 Rechtsgrundlage für die Erteilung von Leitungsnetzauskunft und Schachtschein 2
2.3 Personenbezug bei Leitungsnetzdaten ... 3

3 Datenschutzrechtliche Anforderungen an die Systemgestaltung ... 5
3.1 Allgemeine datenschutzrechtliche Anforderungen ... 5
3.1.1 Rechtmäßigkeit des Umgangs mit personenbezogenen Daten ... 5
3.1.2 Zweckbindung der erhobenen personenbezogenen Daten ... 7
3.1.3 Erforderlichkeit des Umgangs mit personenbezogenen Daten ... 7
3.1.4 Datenvermeidung und Datensparsamkeit ... 8
3.1.5 Transparenz der Datenverarbeitungsprozesse ... 8
3.1.6 Datensicherheit ... 9
3.1.7 Kontrolle der Datenverarbeitungsprozesse ... 9
3.1.7.1 Kontrolle durch den Landesbeauftragten für den Datenschutz ... 10
3.1.7.2 Kontrolle durch den behördlichen Datenschutzbeauftragten ... 10
3.1.7.3 Durchführung eines Datenschutzaudits ... 11
3.1.7.4 Verfahrensverzeichnis ... 11
3.1.7.5 Freigabe und Vorabkontrolle ... 12
3.1.8 Beachtung der Betroffenenrechte ... 12
3.1.8.1 Recht auf Benachrichtigung ... 12
3.1.8.2 Recht auf Auskunft oder Akteneinsicht ... 12
3.1.8.3 Recht auf Berichtigung ... 13
3.1.8.4 Recht auf Löschung ... 14
3.1.8.5 Recht auf Sperrung ... 14
3.1.8.6 Recht auf Widerspruch ... 14
3.1.8.7 Recht auf Schadenersatz ... 15
3.1.8.8 Recht auf Anrufung des Landesdatenschutzbeauftragten ... 15
3.2 Bereichsspezifische datenschutzrechtliche Vorschriften ... 15
3.2.1 Anfallende Daten ... 16
3.2.1.1 Bestandsdaten ... 16
3.2.1.2 Nutzungsdaten ... 17
3.2.1.3 Abrechnungsdaten ... 17
3.2.2 Pflichten des Diensteanbieters ... 17
3.2.2.1 Allgemeine Informationspflichten ... 17
3.2.2.2 Unterrichtungspflicht ... 18
3.2.2.3 Technische und organisatorische Vorkehrungen ... 18
3.2.2.4 Bereitstellung einer anonymen Nutzungsmöglichkeit ... 19
3.2.2.5 Auskunftspflicht ... 19

4 Juristische Betrachtung der Prozesse ... 21
4.1 Verhältnis zwischen Geoportal und datenliefernden Stellen ... 21
4.1.1 Umgang mit unterschiedlichen Nutzungsbestimmungen ... 21
4.1.2 Schutzrechte in Bezug auf Geoinformationen ... 21
4.2 Verhältnis zwischen Geoportal und Nutzer ... 22
4.2.1 Zulässigkeit des Datenabrufs aus dem Portal ... 22
4.2.2 Zugang zum System ... 23

4.2.2.1 Registrierung des Nutzers 23
4.2.2.1.1 Registrierung mittels Postident-Verfahren 24
4.2.2.1.2 Registrierung mittels Elektronischem Personalausweis 24
4.2.2.1.3 Registrierung mittels Bürgerportalen 24
4.2.2.2 Prüfung des berechtigten Interesses und Zuweisung der Nutzerrolle 25
4.2.3 Nutzung des Systems 26
4.2.3.1 Urheberrechtlicher Schutz 26
4.2.3.2 Einbeziehung der „Nutzungsbedingungen für übergebene digitale Bestandspläne“ 27
4.2.4 Abmeldung vom System 29

5 Sicherheits- und haftungsrelevante Aspekte 30
5.1 Sicherheitsanforderungen an den Kommunikationsprozess 30
5.1.1 Vertraulichkeit 30
5.1.2 Verfügbarkeit 31
5.2 Zugesicherte Gültigkeitsdauer der Auskünfte 31
5.3 Elektronische Aufbewahrung zur Beweissicherung 32

1 Fragestellung

Das Projekt „Mobiler Tiefbau-Assistent mit rechtsverbindlicher und sicherer Daten-Aggregation für den Fernzugriff auf ad-hoc integrierbare leitungsnetzbezogene GeoGovernment-Services (TRUFFLE)“ ist ein gemeinsames Forschungsvorhaben des Zweckverbands Grevesmühlen (ZVG), des Fraunhofer IGD Rostock, der Consinto GmbH sowie der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel.

Baumaßnahmen ab einer bestimmten Tiefe gefährden die im Erdreich verlegten Ver- und Entsorgungsleitungen. Um bei Tiefbauarbeiten Schäden zu vermeiden, ist es notwendig, dass dem Bauausführenden vor Beginn der jeweiligen Maßnahme Informationen zur Lage und Art der unterirdischen Infrastruktur vorliegen. Diese müssen gegenwärtig verhältnismäßig aufwändig bei sämtlichen ansässigen Fernwärme-, Gas-, Strom- und Wasserversorgungs- sowie Telekommunikationsunternehmen angefragt werden, von deren Versorgungsgebiet auch das jeweilige Grundstück umfasst ist. Anhaltspunkte dazu liefern z. B. die Listen zu den Trägern öffentlicher Belange, die bei den Kommunen eingesehen werden können.[1]

Ziel des Vorhabens ist die Bereitstellung einer Web-Auskunft, die sich an verschiedene Adressaten, wie Ämter, Planungsbüros und private Bauherrn, richtet. Die Ämter sollen primär die Möglichkeit haben, unkompliziert und tagesaktuell online auf den Leitungsbestand des Versorgungsgebiets Grevesmühlen zugreifen zu können. Etwa für Planungsbüros, Architekten und Privatpersonen soll der Dienst in erster Linie zur Vereinfachung der Beantragung von Schachtscheinen und Leitungsauskünften führen. Ein Schachtschein enthält u. a. die Erlaubnis eines Versorgungsunternehmens, Tiefbauarbeiten auf einem bestimmten Grundstück – unter Einhaltung der in ihm enthaltenen Auflagen (bspw. Notwendigkeit einer der Baumaßnahme vorausgehenden Handschachtung) – durchführen zu dürfen. Demgegenüber stellt eine Leitungsauskunft lediglich eine Information zur Art und Lage von Leitungen und Rohren dar, die lediglich als Planungsgrundlage zu dienen vermag.

Eine besondere datenschutzrechtliche Relevanz im Zusammenhang mit der im Rahmen von TRUFFLE vorgesehenen Online-Auskunft ist einerseits deshalb gegeben, weil die Auskünfte auch grundstückspezifische Angaben enthalten können, die einen Personenbezug aufweisen. Andererseits ist zur Inanspruchnahme des Auskunftsdienstes durch bestimmte Nutzerkategorien eine Identifizierung des Geoportalnutzers notwendig. Somit sind auch hierzu personenbezogene Datenverarbeitungsvorgänge unvermeidbar, die dem Datenschutzrecht unterliegen.

Im Zusammenhang mit den Diensten des Geoportals des ZVG wird zukünftig das Gesetz über das amtliche Geoinformations- und Vermessungswesen Mecklenburg-Vorpommern (GeoVermG M-V) hohe Relevanz erlangen, für das zum Zeitpunkt der Erstellung des vorliegenden Gutachtens der Gesetzentwurf[2] vorliegt. Dieses Gesetz wird spezifische Vorschriften für den Bereich Geoinformationswesen enthalten. Durch die EG-Richtlinie 2007/2/EG (INSPIRE-Richtlinie) sind sowohl Bund und als auch Länder aufgefordert worden, notwendige Rechts- und Verwaltungsvorschriften zu erlassen, um den Zugang zu und die Nutzung von Geodaten für Bürger, Verwaltung und Wirtschaft zu erleichtern. Da sowohl das künftige Landes- als auch das bereits bestehende Geodatenzugangsgesetz des Bundes (GeoZG) der Umsetzung der Richtlinie dienen, kann im Folgenden die amtliche Begründung des GeoZG des Bundes[3] auch zum Verständnis des GeoVermG M-V herangezogen werden.

[1] Bundesverband der Energie- und Wasserwirtschaft e. V., Technischer Hinweis – Erteilung von Auskünften, 4.
[2] LT M-V Drs. 5/3476.
[3] BT-Drs. 16/10530, 1 ff.

2 Grundlagen

2.1 Rechtsstellung des Zweckverbands Grevesmühlen

Der Zweckverband Grevesmühlen (ZVG) ist eine Körperschaft öffentlichen Rechts ohne Gebietshoheit gem. § 10 Abs. 1 LOG M-V und § 1 Abs. 1 Satz 1 ZVG Verbandssatzung. Beim Zweckverband handelt sich um einen verselbständigten und mitgliedschaftlich organisierten rechtsfähigen Verwaltungsträger, der dauerhaft Aufgaben im öffentlichen Interesse wahrnimmt.

Die Aufgaben des ZVG bestehen gem. § 3 Abs. 1 und 2 ZVG Verbandssatzung in der Wasserversorgung, Abwasserbeseitigung, -reinigung sowie der Geodatenerfassung und -nutzung durch Errichtung und Betrieb eines Geodatenfachinformationssystems. Da es sich beim Zweckverband um eine öffentliche Behörde des Landes handelt, sind die einschlägigen Landesgesetze Mecklenburg-Vorpommerns für die rechtliche Beurteilung der Gestaltung des Geoportals heranzuziehen.

2.2 Rechtsgrundlage für die Erteilung von Leitungsnetzauskunft und Schachtschein

Bauordnungsrechtlich sieht § 7 Abs. 3 Nr. 6 BauVorlVO M-V vor, dass der Lageplan im Rahmen der vorzulegenden Bauvorlagen auch Leitungen, die zur öffentlichen Versorgung mit Wasser, Elektrizität, Gas, Wärme, der öffentlichen Abwasserentsorgung oder der Telekommunikation dienen, und Rohrleitungen zum Ferntransport von Stoffen, sowie deren Abstände zur geplanten baulichen Anlage enthalten müssen, soweit dies zur Beurteilung des Bauvorhabens erforderlich ist.

Zivilrechtlich ist es für den Bauherrn, den Bauunternehmer, den Architekten oder den planenden Ingenieur notwendig, eine Leitungsnetzauskunft und einen Schachtschein einzuholen, um Haftungsansprüche zu vermeiden. Aus § 823 BGB folgt eine Verkehrssicherungspflicht für denjenigen, der eine Gefahrenlage schafft. Diese Pflicht umfasst sämtliche notwendigen und zumutbaren Vorkehrungen, um eine Schädigung anderer zu vermeiden. Der notwendige Sorgfaltsmaßstab hat sich an einem umsichtigen und verständigen, in vernünftigem Maße vorsichtigen Menschen zu orientieren. Wenn konkrete Anhaltspunkte für unterirdisch verlegte Versorgungsleitungen auf einem privaten Grundstück gegeben sind, besteht eine allgemeine Pflicht, sich nach diesen Leitungen bei den Energieversorgungsunternehmen zu erkundigen, da Versorgungsleitungen im Regelfall ohne Mitwirken der kommunalen Bauämter verlegt und unterhalten werden. In Bezug auf öffentliche Flächen besteht diese Verpflichtung stets.[4] Die Pflicht zur Einholung der notwendigen Informationen erstreckt sich insbesondere auf die jeweiligen Versorgungsunternehmen, inklusive privater Telekommunikationsunternehmen. Sind in der näheren Umgebung der geplanten Tiefbauarbeiten Gleise verlegt, muss eine Auskunft bei der Deutschen Bahn eingeholt werden.[5]

Aufgrund der enormen Schadenshöhe, die aus der Durchtrennung von Gas- und Starkstromleitungen resultieren kann, sind an die Verpflichtung der Auskunftseinholung strenge Anforderungen zu stellen. Diesbezügliche DIN-Normen („Erdarbeiten“ und „Bauarbeiten“) können dabei als Richtschnur herangezogen werden.[6]

[4] *BGH*, NJW-RR 2006, 674 ff.
[5] MüKo BGB/*Wagner*, 5. Aufl. 2009, § 823 Rn. 479.
[6] MüKo BGB/*Wagner*, 5. Aufl. 2009, § 823 Rn. 479.

Die Auskunftsverpflichtung der Versorgungsunternehmen, die für die Infrastrukturleitungen zuständig sind, ergibt sich aus einem möglichen Mitverschulden, wenn sie die Auskunft verweigern. § 254 BGB macht die Verantwortlichkeit des Geschädigten von seinem Verhalten in Bezug auf die Entstehung des Schadens abhängig.[7] Die Vorschrift begründet u. U. ein Mitverschulden des Versorgungsunternehmens, wenn es dem Auskunftsbegehren nicht oder nicht in geeigneter oder ausreichender Form nachkommt.

Einzelfallabhängig, und je nach Art des Versorgungsunternehmens, können sich Haftungsansprüche gegen das Unternehmen insbesondere auch aus § 823 Abs. 2 BGB, § 2 Abs. 1 HaftPflG, § 6 AVBWasserV, § 18 NDAV, § 18 NAV sowie aus den Vorschriften des UmweltHG ergeben.

Darüber hinaus wird der unbeschadete Bestand und Schutz der eigenen Leitungsinfrastruktur im Interesse eines jeden Versorgungsunternehmens liegen. Schon allein aus diesem Grund ist es für das Versorgungsunternehmen sinnvoll, leitungsbezogene Auskünfte unter Einhaltung großer Sorgfalt zu erteilen. Um dem gerecht zu werden, sind ein hoher Detailliertheitsgrad, gute Lesbarkeit und Verständlichkeit, Aktualität sowie Vollständigkeit der in den Auskünften enthaltenen Informationen zu gewährleisten.

2.3 Personenbezug bei Leitungsnetzdaten

Das Datenschutzrecht ist zu beachten, wenn ein Umgang mit personenbezogenen Daten erfolgt. Liegt ein Personenbezug der Daten vor, findet gegenüber einer öffentlich-rechtlichen Körperschaft eines Landes wie dem Zweckverband Grevesmühlen in erster Linie das Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) Anwendung.

Ein „Personenbezug“ liegt gem. § 3 Abs. 1 DSG M-V vor, wenn Daten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person enthalten. Die Daten müssen also irgendeinen Bezug zu einer Person aufweisen. Das im Volkszählungsurteil[8] konstruierte Recht auf informationelle Selbstbestimmung enthält u. a. die Aussage, dass kein belangloses personenbezogenes Datum existiert; insofern gelten die Datenschutzregeln grundsätzlich für jegliche Information, die mit einer Person in Verbindung gebracht werden kann.

Für den Betreiber des Geoportals stellen die Infrastrukturdaten über Leitungsnetze – zumindest mittelbar – personenbezogene Daten dar. Da grundstücksbezogene Auskünfte durch das Geoportal realisiert werden sollen, muss dem Geoportal die Zuordnung des Leitungsbestands zum jeweiligen Grundstück bekannt sein. Da jedes Grundstück einem Eigentümer zugeordnet werden kann, liegen dem Geoportal zumindest in Bezug auf jeden privaten Grundstückseigentümer personenbezogene Daten vor.[9] Auch die Möglichkeit, dass Grundstückseigentümer selbst Auskünfte über die unter ihrem Grundstück verlegten Leitungen einholen können, bedingt, dass beim Geoportalbetreiber die Zuordnung von Grundstückseigentümer zum entsprechenden Grundstück bekannt sein muss; das Geoportal hat bei Auskünften für Privatpersonen zu prüfen, ob ein berechtigtes Interesse zur Einsichtnahme der Informationen vorliegt. Über die Melderegister der Einwohnermeldeämter sind darüber hinaus auch sämtliche weiteren auf dem betreffenden Grundstück lebenden Personen ermittelbar; gem. § 11 Abs. 1 MRRG haben

[7] BeckOK BGB/*Unberath*, Ed. 18, Stand 1.2.2007, § 254 Rn. 1.
[8] *BVerfG* 15.12.1983, NJW 1984, 419.
[9] Ebenso *Ziegler*, NVwZ 1993, 347 sowie *Jahn/Striezel*, K&R 2009, 753 (755).

sich alle Personen, die eine Wohnung beziehen, bei der jeweiligen Meldebehörde anzumelden.

Beim Leitungsbestand eines bestimmten Grundstücks kann es sich auch für Dritte um personenbezogene Daten handeln, wenn sie die Zuordnung des Grundstücks zum Eigentümer kennen. Wenn beispielsweise Nachbarn gegenseitig Einblick in den Bestand des jeweils anderen Nachbarn nehmen können, sind die einsehbaren Leitungsinformationen für sie personenbezogen.

Da der Umgang mit personenbezogenen Daten dem Datenschutzrecht unterliegt, müssen einschlägige Rechtsvorschriften zu deren Schutz eingehalten werden.

3 Datenschutzrechtliche Anforderungen an die Systemgestaltung

3.1 Allgemeine datenschutzrechtliche Anforderungen

Das im Rahmen des Projekts TRUFFLE zur Anwendung kommende technische System bedingt, dass in vielfacher Hinsicht personenbezogene Daten automatisch erhoben, verarbeitet und genutzt werden; dies hat zur Folge, dass die Vorschriften des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) Beachtung finden müssen.

Das Landesdatenschutzgesetz Mecklenburg-Vorpommern hat gem. § 1 DSG M-V den Zweck, das Recht des Einzelnen zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen zu können. Die aus dem Blickwinkel des Datenschutzes im Projekt TRUFFLE Relevanz erlangenden Aspekte werden nachfolgend den datenschutzrechtlichen Grundsätzen zugeordnet und kurz erläutert. Die Realisierung dieser Grundsätze stellt die Anforderungsstruktur an TRUFFLE dar.

3.1.1 Rechtmäßigkeit des Umgangs mit personenbezogenen Daten

Im Gegensatz zum Bereich der privaten Rechtsbeziehungen, wo privatautonom Vereinbarungen ausgehandelt werden können, kann sich der Umgang mit personenbezogenen Daten im öffentlichen Bereich in der Regel nicht am Grundsatz des freien Willens des Betroffenen orientieren. Die Befugnisse der Behörden ergeben sich durch gesetzliche Regelungen.[10]

Um personenbezogene Datenverarbeitungsvorgänge zulässig durchführen zu können, wird gem. § 7 Abs. 1 DSG M-V eine Erlaubnisnorm oder eine Einwilligung des Betroffenen benötigt. Betroffener kann gem. § 3 Abs. 1 DSG M-V nur eine natürliche Person sein, die bestimmt oder zumindest bestimmbar ist. Welche Aktivitäten unter eine personenbezogene Datenverarbeitung fallen, ist in § 3 Abs. 4 Satz 1, 2 Nr. 1 bis 10 DSG M-V aufgeführt. Die Vorgänge des

- Erhebens,
- Speicherns,
- Veränderns,
- Übermittelns,
- Sperrens,
- Löschens,
- Nutzens,
- Anonymisierens,
- Pseudonymisierens,
- Verschlüsselns

von personenbezogenen Daten erfüllen die Voraussetzungen.

§ 9 Abs. 2 DSG M-V fordert, personenbezogene Daten grundsätzlich nur beim Betroffenen selbst und mit seiner Kenntnis zu erheben. Der Betroffene soll stets wissen, wer welche Daten wann und wofür über seine Person sammelt, speichert und verarbeitet.[11] Ausnahmen vom

[10] *Roßnagel/Laue*, in: Roßnagel/Laue/Peters (Hrsg.), Delegation von Aufgaben an IT-Assistenzsysteme, 2009, 29.
[11] *Gola*, in: Gola/Schomerus, BDSG, 9. Aufl. 2007, § 4 Rn. 21.

Grundsatz der Direkterhebung können sich aus Rechtsvorschriften, die eine andere Art der Erhebung zulassen oder voraussetzen, oder einer entsprechenden Einwilligung ergeben.

Die Erlaubnis zu den bezeichneten Datenverarbeitungen kann sich gem. § 7 Abs. 1 DSG M-V entweder aus dem DSG M-V selbst, einer anderen Rechtsvorschrift oder einer Einwilligung des Betroffenen ergeben. Fallen die betreffenden Daten in den Bereich der besonders schutzwürdigen Daten gem. § 7 Abs. 2 DSG M-V (Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben), hat sich die Beurteilung über deren Verarbeitungsbefugnis an strengen Maßstäben zu orientieren, §§ 7 Abs. 2 und 3, 8 Abs. 1 Satz 2 DSG M-V. Die sensitiven Daten bergen ein erhebliches Risiko für den Betroffenen – ihre missbräuchliche Nutzung kann gravierende Folgen für die betreffende Person nach sich ziehen. Ferner lassen sich auf der Grundlage der gewonnenen Daten Vermutungen hinsichtlich der Privat- und Intimsphäre der Person anstellen.

Ganz allgemein erlangt eine Einwilligung gem. § 8 Abs. 1 DSG M-V nur dann Wirksamkeit, wenn sie freiwillig abgegeben wurde. Darüber hinaus ist sie im Regelfall schriftlich zu erteilen und muss die Art und den Umfang der Verarbeitung, die datenverarbeitende Stelle und die potenziellen Empfänger der Daten sowie die Folgen einer verweigerten Einwilligung erkennen lassen. Der Betroffene muss darauf hingewiesen werden, dass er die Einwilligung widerrufen kann. Wenn sie zusammen mit anderen Erklärungen abgegeben werden soll, ist eine besondere Hervorhebung erforderlich. Abs. 2 lässt ausdrücklich die elektronische Einwilligung zu.

Besondere Regelungen für die Übermittlung von Geodaten enthält das GeoVermG M-V, nach dessen § 14 Geodaten und Geodatendienste öffentlich verfügbar zu machen sind. Die Vorschrift sieht weitergehend für Darstellungsdienste vor, dass die Bereitstellung der Geodaten derart erfolgen kann, dass eine Weiterverwendung – insbesondere zur kommerziellen Nutzung – ausgeschlossen ist. Das Geoportal verkörpert einen solchen Darstellungsdienst, deshalb darf es von dieser Ausschlussmöglichkeit Gebrauch machen.

In § 15 GeoVermG M-V sind Restriktionen für den Zugang zu Geodaten verankert. Gem. § 15 Abs. 2 Satz 2 Nr. 1 GeoVermG M-V ist der Zugang zu Geoinformationen insoweit zu beschränken, als personenbezogene Daten offenbart würden und damit eine Beeinträchtigung von schutzwürdigen Interessen der Betroffenen einherginge, es sei denn von diesen liegt eine diesbezügliche Einwilligung vor. Ob der Zugang zu personenbezogenen Geodaten – ohne den generell unpraktikablen Umweg über die Einwilligung – eröffnet werden kann, hängt maßgeblich davon ab, ob schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

§ 14 GeoVermG M-V regelt die Bereitstellung von Geobasisdaten. Die vom Landkreis Nordwestmecklenburg übertragenen Daten der Automatisierten Liegenschaftskarte (ALK) und des Automatisierten Liegenschaftsbuchs (ALB) stellen Geobasisdaten im Sinne der Vorschrift dar. Die ALK-Daten bilden den vermessungs- und kartentechnischen Teil des Liegenschaftskatasters; der beschreibende Teil besteht im ALB.[12]

Darüber hinaus bestimmt Abs. 4 des § 15 GeoVermG M-V, dass die Bereitstellung von personenbezogenen Geodaten stets unter Beachtung der datenschutzrechtlichen Grundsätze des Landesdatenschutzgesetzes sowie des Bundesdatenschutzgesetzes zu erfolgen hat. Neben der Frage der Zulässigkeit der Verarbeitung personenbezogener Daten sind daher für die Durch-

[12] Themenrundgang amtliche Geobasisdaten (abrufbar unter: http://www.geoinformatik.uni-rostock.de/rundgangeinzel.asp?ID=1).

führung der Datenerhebung, -verarbeitung und -nutzung die folgenden Grundsätze zu beachten.

3.1.2 Zweckbindung der erhobenen personenbezogenen Daten

Das DSG M-V enthält das grundsätzliche Erfordernis, dass personenbezogene Daten nur zu vorab festgelegten Zwecken erhoben, verarbeitet und genutzt werden dürfen. Der Betroffene ist gem. § 9 Abs. 3 Satz 1 DSG M-V u. a. über die Zwecke in Kenntnis zu setzen, wenn er von der Datenerhebung noch keine Kenntnis hat. Der Umgang mit den Daten darf sich gem. §§ 10 Abs. 2 Satz 1 und 11 Abs. 2 DSG M-V nach Festlegung des Zwecks nur innerhalb dieser Zweckbestimmung vollziehen, d. h. eine geplante Zweckänderung erfordert nach § 10 Abs. 3 DSG M-V im Regelfall eine entsprechende Erlaubnis. Der ausnahmsweise Umgang mit den Daten ist beispielsweise dann zulässig, wenn eine diesbezügliche Einwilligung des Betroffenen vorliegt, sich die Legitimation aus einer Rechtsvorschrift ergibt oder damit schwerwiegende Beeinträchtigungen der Rechte anderer Personen abgewehrt werden können.

§ 10 Abs. 6 DSG M-V enthält eine Bestimmung, die eine besondere Zweckbindung von personenbezogenen Daten zur Datenschutzkontrolle, zur Datensicherheit sowie zur Sicherstellung des ordnungsgemäßen Betriebs von Datenverarbeitungsanlagen vorsieht.

Für das Geoportal des ZVG bedeutet dies konkret, dass sämtliche personenbezogenen Daten, die zur Durchführung des Vertrags mit dem Nutzer notwendig sind, und daher erhoben werden müssen, nur zum Zweck der Vertragsabwicklung genutzt werden dürfen. Eine andere Nutzung der Daten, etwa zur Information des Kunden über neue Leistungen des ZVG, sind damit unzulässig.

Die Zweckbegrenzung und -bindung sind primär durch eine entsprechende Systemgestaltung und den Systemdatenschutz sicherzustellen.[13]

3.1.3 Erforderlichkeit des Umgangs mit personenbezogenen Daten

Erforderlich ist der Umgang mit personenbezogenen Daten nur dann, wenn er für die Erfüllung des zulässigen Zwecks unentbehrlich ist.[14] Eignet sich ein Datum zwar zur Erfüllung der angestrebten Aufgabe oder ist es für sie zweckdienlich, liegt noch nicht die notwendige Erforderlichkeit vor. Die Geeignetheit des Datums allein stellt nur die notwendige, nicht jedoch die hinreichende Bedingung zum Vorliegen der Erforderlichkeit dar.[15] Dabei bezieht sich die Erforderlichkeit des Datenumgangs auf ein bestimmtes technisches System sowie einen gegebenen Datenverarbeitungsprozess. Sie verkörpert eine normative Zweck-Mittel-Beziehung. Die Grundlage für einen zulässigen Zweck der personenbezogenen Datenverarbeitung bildet ihre Legitimation, die sich etwa aus einer gesetzlichen Anordnung oder Befugnis ergeben kann.[16]

Um dem Prinzip der Erforderlichkeit zu genügen, ist der Umgang mit den personenbezogenen Daten beim Geoportal unter Einhaltung der nachfolgend aufgeführten Forderungen zu vollziehen:

[13] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 71.
[14] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 69.
[15] *Roßnagel*, Modernisierung des Datenschutzrechts, 2001, 98.
[16] *Roßnagel*, Modernisierung des Datenschutzrechts, 2001, 98 ff.

- Nur die zur Erreichung des festgelegten Zwecks unverzichtbaren Daten dürfen verarbeitet werden. Eine Speicherung von personenbezogenen Daten auf Vorrat zur Verwendung für sich potenziell zukünftig ergebende Zwecke ist verboten.
- Im Rahmen der Datenverarbeitung dürfen personenbezogene Daten nur in denjenigen Phasen verwendet werden, die zur Erreichung des festgelegten Zwecks notwendig sind. So ist es etwa verboten, Daten zu speichern, wenn lediglich ihre Erhebung für das Erreichen der Zwecke ausreicht.
- Der Umgang mit den personenbezogenen Daten darf nur innerhalb des Zeitraums stattfinden, in dem sie für die Zweckerreichung benötigt werden. Danach sind sie frühest möglich zu löschen.[17]

3.1.4 Datenvermeidung und Datensparsamkeit

§ 5 Abs. 1 DSG M-V normiert eines der obersten Gebote des Datenschutzrechts, nämlich die Datenvermeidung. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten soll möglichst so gestaltet sein, dass personenbezogene Daten überhaupt nicht verwendet werden. Ist es nicht realisierbar, den Zweck der Datenverarbeitung auch ohne Personenbezug zu erreichen, sollen so wenig wie möglich personenbezogene Daten verarbeitet werden. Sofern der Umgang mit personenbezogenen Daten für das Funktionieren des Systems unumgänglich ist, sind die Prozesse vorzugsweise so zu gestalten, dass die Verarbeitung dieser Daten möglichst kurz gehalten wird und die Daten frühest möglich gelöscht, anonymisiert oder pseudonymisiert werden.[18]

Eine grundsätzliche Möglichkeit der Datenvermeidung besteht in der Anonymisierung der Person, über die Informationen verarbeitet werden. Die Anonymisierungsmethode kann überall dort eingesetzt werden, wo es auf die tatsächliche Identität einer Person nicht ankommt. Anonymes Handeln ist beispielsweise dort denkbar, wo lediglich Informationen abgefragt oder getauscht werden sollen.[19]

Auch mit der Pseudonymisierung lässt sich das informationelle Selbstbestimmungsrecht des Betroffenen wahren. Pseudonymität bedeutet, dass der Nutzer ein Kennzeichen verwendet, durch das die Wahrscheinlichkeit der Zuordnung von Daten zu seiner Person ohne Kenntnis der Zuordnungsregel derart gering ist, dass sie nach Lebenserfahrung und dem Stand der Wissenschaft praktisch ausscheidet. Bei der Pseudonymität existiert stets eine Regel, über die der Betroffene dem Pseudonym zugeordnet werden kann. Daten zu einem Pseudonym lassen sich miteinander verknüpfen; so ist es möglich, umfassende Profile zu erstellen, die eine Wiedererkennung ohne die Identifizierung der hinter dem Pseudonym stehenden Person erlauben.[20] Möglichkeiten einer anonymen und pseudonymen Nutzung der Online-Auskunft werden im Kapitelunterpunkt 3.2.2.4, Bereitstellung einer anonymen Nutzungsmöglichkeit, geprüft.

3.1.5 Transparenz der Datenverarbeitungsprozesse

Die Notwendigkeit des transparenten Umgangs mit personenbezogenen Daten ergibt sich insbesondere aus der Tatsache, dass diese Daten für den Betroffenen unbemerkt erhoben, verarbeitet und genutzt werden können.

[17] *Roßnagel*, Modernisierung des Datenschutzrechts, 2001, 98 f.
[18] *Roßnagel*, Modernisierung des Datenschutzrechts, 2001, 101.
[19] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 58.
[20] *Roßnagel*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4 Rn. 60 ff.

Zur Herstellung der erforderlichen Transparenz dient vor allem die bereits erwähnte Datenerhebung beim Betroffenen. Außerdem sieht das DSG M-V zwei weitere Formen der Transparenzsicherung vor:

1. Informationspflichten für die datenverarbeitende Stelle, wobei die Stelle selbst aktiv werden muss (Pflicht zur Benachrichtigung Betroffener, § 23 DSG M-V) und
2. Auskunftsansprüche des Betroffenen, für dessen Durchsetzung der Betroffene verantwortlich ist (Auskunft, Akteneinsicht, § 24 DSG M-V).

In diesem Zusammenhang darf der potenzielle Akzeptanzgewinn hinsichtlich der Datenverarbeitung beim Betroffenen nicht unterschätzt werden: Wenn ihm bereits im Vorfeld verdeutlicht wird, für welche Zwecke und wie seine personenbezogenen Daten verarbeitet werden, vermag dies u. U. zu einer höheren Bereitschaft führen, solche Daten bereitzustellen.

Die dargestellten Informationsrechte des Betroffenen stellen sog. Betroffenenrechte im Sinne des Kapitelunterpunkts 3.1.8 dar und werden deshalb aus Gründen der besseren Übersichtlichkeit dort erläutert.

3.1.6 Datensicherheit

Die §§ 21 und 22 DSG M-V enthalten Ausführungen zu technischen und organisatorischen Maßnahmen, die allgemein bei personenbezogener Datenverarbeitung und insbesondere bei automatisierter personenbezogener Datenverarbeitung ergriffen werden müssen. Die technischen und organisatorischen Voraussetzungen sind vom Geoportal zu erfüllen.

§ 21 DSG M-V fordert in Bezug auf die allgemeinen Maßnahmen zur Datensicherheit insbesondere die nachfolgend aufgezeigten Vorkehrungen; es müssen solche Maßnahmen eingeleitet werden, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Primär ist sicherzustellen, dass

- nur autorisierte Personen Daten mit Personenbezug einsehen können;
- die Unversehrtheit, Vollständigkeit und Aktualität der personenbezogenen Daten während des Verarbeitungsvorgangs gewahrt bleiben;
- die rechtzeitige Verfügbarkeit und ordnungsgemäße Verarbeitung der personenbezogenen Daten gewährleistet ist;
- die Zuordnung zum Ursprung der personenbezogenen Daten jederzeit möglich ist;
- ein Protokollierungsverfahren eingerichtet wird;
- die Nachvollziehbarkeit der personenbezogenen Datenverarbeitungsvorgänge gegeben ist.

§ 22 DSG M-V fordert besondere Maßnahmen zur Herstellung der Datensicherheit bei automatisierten Verfahren. Dies betrifft Berechtigungserfordernisse, Zugriffs- und Kontrollpflichten, Notwendigkeit der Verschlüsselung und das Aufstellen eines Sicherheitskonzepts.

3.1.7 Kontrolle der Datenverarbeitungsprozesse

Generell sieht der Gesetzgeber für Tätigkeiten, von denen potenziell Gefahren für den Einzelnen oder die Allgemeinheit ausgehen, Kontrollen vor – so auch für den Bereich des Datenschutzes. Nachstehend werden die Kontrollorgane für öffentliche Stellen des Landes kurz

vorgestellt sowie weitere obligatorische und fakultative Verfahren, die der Überprüfung dienen, ob die Vorschriften zum Datenschutz eingehalten werden. Das Geoportal unterliegt der Kontrolle der nachstehend aufgezeigten Überwachungsinstitutionen.

3.1.7.1 Kontrolle durch den Landesbeauftragten für den Datenschutz

Als datenschutzrechtliches Kontrollorgan für öffentliche Stellen, die in den Anwendungsbereich des DSG M-V fallen und Daten verarbeiten, fungiert der Landesbeauftragte für den Datenschutz. Seine Stellung, Aufgaben und Kompetenzen sind in den §§ 29 bis 33a DSG M-V reglementiert.[21]

Der Landesbeauftragte für den Datenschutz arbeitet nach dem sog. Kooperationsprinzip, d. h. in enger Zusammenarbeit mit behördlichen Datenschutzbeauftragten. Gem. § 29 Abs. 6 Satz 1 DSG M-V ist der Landesdatenschutzbeauftragte in seiner Aufgabenerfüllung unabhängig und nur dem Gesetz unterworfen.

Gem. § 30 Abs. 1 DSG M-V ist die primäre Aufgabe des Kontrollorgans, die Ausführung des DSG M-V sowie anderer datenschutzrechtlicher Vorschriften bei öffentlichen Stellen zu überwachen. Aus diesem Auftrag ergeben sich für ihn die Funktionen

- Beschwerdemanagement,
- Kontrolle,
- Beanstandung,
- Mängelbeseitigung,
- Beratung und
- Information von Betroffenen und der Öffentlichkeit.

Die öffentlichen Stellen, die der Kontrolle durch den Landesdatenschutzbeauftragten unterliegen, sind aus § 31 Abs. 1 DSG M-V verpflichtet, ihn zu unterstützen; daraus resultieren insbesondere die Pflichten, ihm Auskünfte zu geben, Einsicht in Unterlagen zu gewähren sowie ihm jederzeit Zutritt zu den Diensträumen zu ermöglichen.

3.1.7.2 Kontrolle durch den behördlichen Datenschutzbeauftragten

Sämtliche öffentliche Stellen, die in den Anwendungsbereich des Landesdatenschutzgesetzes M-V fallen und Daten verarbeiten – somit auch das Geoportal des ZVG –, unterliegen gem. § 20 Abs. 1 Satz 1 DSG M-V der Verpflichtung, einen behördlichen Datenschutzbeauftragen, inklusive Vertreter, schriftlich[22] zu bestellen. Vorzugsweise soll der Datenschutzbeauftragte Beschäftigter der datenverarbeitenden Stelle sein. Er muss insbesondere über die erforderliche Sachkunde und Zuverlässigkeit verfügen. Der behördliche Beauftragte für den Datenschutz ist dem Leiter der Stelle direkt unterstellt und in der Ausführung seiner Aufgabe unabhängig und weisungsfrei.

Eine solche innerbehördliche Selbstkontrolle durch die Person des Datenschutzbeauftragten soll insbesondere der Entlastung staatlicher Aufsichtsorgane dienen.[23] Der Beauftragte für

[21] *Hillenbrand-Beck*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.4 Rn. 1.
[22] Musterformular zur Bestellung eines behördlichen Datenschutzbeauftragten abrufbar unter: http://www.lfd.m-v.de/navi/dschutz/behdsb.html.
[23] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 1.

Datenschutz sorgt in der öffentlichen Stelle für die Umsetzung und Einhaltung der Vorschriften des Landesdatenschutzgesetzes sowie weiterer datenschutzrechtlicher Vorschriften.

Der behördliche Datenschutzbeauftragte nimmt im Wesentlichen

- Kontrollaufgaben,
- Beratungsaufgaben,
- Schulungsaufgaben und
- Registeraufgaben

wahr.[24]

Besonders im Hinblick auf die Umsetzung der in Unterpunkt 3.1.6 genannten Datensicherheitsmaßnahmen drängt sich die Frage auf, ob hierfür nicht ein spezialisierter IT-Sicherheitsbeauftragter hinzugezogen werden sollte. Diese Tätigkeit können externe Dienstleister oder innerbebehördliche Personen wahrnehmen. Eine gesetzliche Pflicht zur Bestellung eines solchen Funktionsträgers besteht im Zusammenhang mit TRUFFLE – im Gegensatz zur Bestellung des Datenschutzbeauftragten – allerdings nicht.

3.1.7.3 Durchführung eines Datenschutzaudits

Ein Datenschutzaudit, welches zur Verbesserung des Datenschutzes und der Datensicherheit dienen soll, kann als werbewirksames „Gütesiegel“ eingesetzt werden. Gem. § 5 Abs. 2 DSG M-V sollen solche informationstechnischen Systeme, die im Rahmen eines Prüfverfahrens als mit dem Datenschutz vereinbar und als Datensicherheit gewährleistend eingestuft wurden, vorrangig zum Einsatz gelangen. Ein datenschutzrechtliches Gütesiegel, mit dem der ZVG an die Öffentlichkeit treten könnte, würde zu einer gesteigerten Akzeptanz in der Bevölkerung und bei potenziellen Nutzern des Geoportals beitragen.

3.1.7.4 Verfahrensverzeichnis

Das Geoportal muss dem behördlichen Datenschutzbeauftragten gem. § 18 Abs. 1 DSG M-V eine Beschreibung sämtlicher eingesetzter Datenverarbeitungsverfahren bereitstellen. Der Beauftragte für den Datenschutz hat auf Grundlage dieser Angaben das sog. Verfahrensverzeichnis zu führen. Aus Abs. 2 geht hervor, dass das Verfahrensverzeichnis kontinuierlich zu aktualisieren und nach Aufforderung dem Landesbeauftragten für den Datenschutz bereitzustellen ist.

§ 18 Abs. 1 Nr. 1 bis 7 DSG M-V enthält die zwingenden Inhalte der Verfahrensbeschreibung. Beispielsweise sind Bezeichnung des jeweiligen Verfahrens sowie der verantwortlichen Stelle, Zweckbestimmung der Datenverarbeitung, Rechtsgrundlage sowie Empfängerkreis der Daten mit aufzunehmen.

Gem. § 20 Abs. 4 DSG M-V muss jedermann Einsicht in das Verfahrensverzeichnis gewährt werden; das Recht auf Einsichtnahme erstreckt sich nicht auf getroffene Maßnahmen zur Herstellung von Datensicherheit und nicht auf bestimmte Verfahren, für welche keine Auskunftspflicht besteht.

[24] *Königshofen*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 5.5 Rn. 19 ff.

3.1.7.5 Freigabe und Vorabkontrolle

Durch § 19 Abs. 1 DSG M-V ist festgelegt, dass die Einrichtung oder wesentliche Änderung eines automatisierten Verfahrens zur personenbezogenen Datenverarbeitung der schriftlichen Freigabe durch den Leiter der verantwortlichen Stelle oder dessen Vertreter bedarf.

Das Erfordernis der sog. Vorabkontrolle ist in Abs. 2 verankert: Bevor automatisierte Datenverarbeitungsverfahren eingeführt oder geändert werden, muss der behördliche Beauftragte für den Datenschutz diese Prozesse in festgelegten Fällen auf ihre Zulässigkeit und auf Datensicherheit hin überprüfen. Notwendig ist die Vorabkontrolle bei Verbund- oder Abrufverfahren sowie wenn besondere Arten personenbezogener Daten gem. § 7 Abs. 2 DSG M-V von der Datenverarbeitung betroffen sind.

Sowohl die Einholung der Freigabe als auch die Durchführung der Vorabkontrolle sind vor erstmaliger Inbetriebnahme des Geoportals und vor dessen Wiederinbetriebnahme nach Umsetzung wesentlicher Änderungen erforderlich.

3.1.8 Beachtung der Betroffenenrechte

Werden personenbezogene Daten des Betroffenen erhoben, verarbeitet oder genutzt, stehen diesem verschiedene Ansprüche zu, die der Wahrung seines informationellen Selbstbestimmungsrechts dienen. Damit der Betroffene überhaupt von diesen Rechten Gebrauch machen kann, muss er zunächst vom Umgang mit seinen personenbezogenen Daten wissen. Insofern stellen seine Rechte auf Benachrichtigung und Auskunft wichtige Grundvoraussetzungen zur Wahrnehmung von Einwirkungsrechten dar, wie dem Recht auf Löschung, wenn ein unzutreffender, unrichtiger oder missbräuchlicher Umgang mit seinen Daten stattfindet.[25] Die Betroffenenrechte stehen den Nutzern des Geoportals zu.

Gem. § 28 DSG M-V handelt es sich bei den in §§ 24 bis 27 DSG M-V sämtlich um unabdingbare Rechte des Betroffenen, d. h. ein Ausschluss oder eine Beschränkung kann selbst auf Grundlage einer entsprechenden Einwilligung nicht herbeigeführt werden.

3.1.8.1 Recht auf Benachrichtigung

Eine Informationspflicht der datenverarbeitenden Stelle kommt in § 23 DSG M-V zum Ausdruck: Falls das Geoportal Grund zur Annahme oder Kenntnis hat, dass die Nutzung unrichtiger, unzulässig erhobener oder unzulässig gespeicherter personenbezogener Daten in einer solchen Weise erfolgte, dass daraus Nachteile für den Betroffenen resultieren oder zu resultieren drohen, ist er unverzüglich zu benachrichtigen.

3.1.8.2 Recht auf Auskunft oder Akteneinsicht

Auskunftsansprüche des Betroffenen sind in § 24 DSG M-V manifestiert. Er kann sich auf Antrag beim Geoportal Auskünfte über

- die zu seiner Person gespeicherten Daten,

[25] *Wedde*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.4 Rn. 12 ff.

- die Herkunft und potenzielle Empfänger der Daten,
- den Verarbeitungszweck und die Rechtsgrundlage dafür sowie
- den Ablauf eines automatisierten Verfahrens zur Einzelentscheidung gem. § 12 DSG M-V

erteilen lassen.

Der Antrag des Betroffenen soll die personenbezogenen Daten, über die er Auskunft begehrt, näher beschreiben, insbesondere wenn sie in Akten gespeichert sind. Grund hierfür liegt in der erleichterten Auffindbarkeit. Das Verfahren und die Form der Auskunftserteilung kann die verantwortliche Stelle im Rahmen des pflichtgemäßen Ermessens selbst bestimmen.

Anstatt einer Auskunftserteilung an den Betroffenen kann ihm gem. § 24 Abs. 3 Satz 1 DSG M-V unter bestimmten Voraussetzungen Akteneinsicht gewährt werden. Wann die Auskunft oder Einsicht nicht erteilt werden darf, regelt Abs. 4. Sowohl die Auskunftserteilung als auch die Bereitstellung der Möglichkeit zur Einsichtnahme sind gem. Abs. 7 vom Geoportal unentgeltlich durchzuführen.

Damit dem Auskunftsbegehren von Nutzern zeitnah Rechnung getragen werden kann, sollte das Geoportal durch geeignete technische und organisatorische Vorkehrungen sicherstellen, dass die dafür notwendigen Daten ohne Aufwand vollständig auffindbar sind.

3.1.8.3 Recht auf Berichtigung

Die Berichtigung unrichtiger personenbezogener Daten ist durch § 13 Abs. 1 DSG M-V vorgeschrieben. Als notwendig erweist sich der Berichtigungsanspruch deshalb, weil die Speicherung unrichtiger personenbezogener Daten beim Geoportal das informationelle Selbstbestimmungsrecht des Betroffenen massiv verletzen kann.

Der Begriff „unrichtig“ umfasst sämtliche Fälle, in denen personenbezogene Informationen gespeichert werden, die mit der Realität nicht übereinstimmen; dies bedeutet konkret, dass sowohl falsche (beispielsweise ein nicht zutreffendes Geburtsdatum) als auch unvollständige Angaben darunter zu subsumieren sind.[26]

§ 13 Abs. 1 Satz 2 DSG M-V bestimmt für die Korrektur von personenbezogenen Daten in nicht-automatisierten Dateien oder Akten, dass sie zu kennzeichnen sind, wann und weshalb sie unrichtig waren oder geworden sind. Aus Satz 3 resultiert eine Ergänzungspflicht für personenbezogene Daten, wenn dies durch den Zweck der Speicherung oder berechtigte Interessen des Betroffenen erforderlich wird. Sämtliche Empfänger von berichtigten Daten sind nach § 13 Abs. 7 DSG M-V über deren Korrektur zu informieren, es sei denn, die Benachrichtigung bedeutet einen unverhältnismäßigen Aufwand und es ist anzunehmen, dass keine schutzwürdigen Interessen des Betroffenen beeinträchtigt werden.

[26] *Wedde*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.4 Rn. 55 ff.

3.1.8.4 Recht auf Löschung

§ 13 Abs. 2 DSG M-V enthält einen Anspruch auf Löschung der Daten, falls einer der enumerativ aufgezählten Sachverhalte vorliegt. Unter dem Vorgang der Löschung ist das Unkenntlichmachen gespeicherter personenbezogener Daten zu verstehen.

Die Löschung von Daten beim Geoportal ist durchzuführen, wenn

- sie unrichtig sind und das Geoportal keine Möglichkeit besitzt, sie richtigzustellen,
- sie unzulässig erhoben wurden,
- sie unzulässig gespeichert wurden,
- die Speicherung der personenbezogenen Daten zur Erfüllung des Zwecks, wofür sie erhoben wurden, nicht mehr erforderlich ist.

Erfolgt eine Löschung solcher Daten, müssen andere Stellen, die diese Daten ebenfalls verarbeiten, gem. § 13 Abs. 7 DSG M-V darüber benachrichtigt werden. Nicht notwendig ist diese Information, wenn sie einen unverhältnismäßigen Aufwand darstellt und keine Beeinträchtigung schutzwürdiger Interessen des Betroffenen zu befürchten ist.

3.1.8.5 Recht auf Sperrung

Der Begriff des Sperrens beinhaltet die Kennzeichnung gespeicherter personenbezogener Daten, um deren weitere Verarbeitung oder Nutzung zu beschränken. Gem. § 13 Abs. 3 DSG M-V sind die Daten durch das Geoportal zu sperren anstatt zu berichtigen oder zu löschen, wenn bestimmte Voraussetzungen erfüllt sind. Eine Sperrung hat etwa zu erfolgen, wenn eine Beeinträchtigung schutzwürdiger Interessen durch Berichtigung oder Löschung zu befürchten, oder eine Löschung aufgrund der besonderen Art der Speicherung nicht oder nur mit einem unverhältnismäßigen Aufwand zu bewerkstelligen wäre. § 13 Abs. 5 DSG M-V bestimmt u. a. eine gesonderte Speicherungspflicht für gesperrte Daten; wo dies nicht möglich ist, müssen die entsprechenden Daten besonders vermerkt werden.

Die Benachrichtigung anderer Stellen über die Sperrung der Daten ist durch die Vorschrift des § 13 Abs. 7 DSG M-V vorgesehen. Ausnahmsweise kann von der Unterrichtung abgesehen werden, wenn sie einen unverhältnismäßigen Aufwand darstellt und keine Beeinträchtigung schutzwürdiger Interessen des Betroffenen zu erwarten ist.

Der Sperrungsanspruch des Betroffenen ist explizit in § 25 Abs. 1 und 2 DSG M-V geregelt: Für den Fall, dass der Betroffene die Richtigkeit der Daten bestreitet, ist eine Sperrung vorzunehmen, wenn weder deren Richtigkeit, noch deren Unrichtigkeit ermittelt werden kann. Im Zusammenhang mit der Feststellung eines Schadenersatzanspruchs kann der Betroffene beim Geoportal beantragen, unrichtige, unzulässig erhobene und/oder unzulässig gespeicherte Daten zu sperren.

3.1.8.6 Recht auf Widerspruch

Ein weiteres Einwirkungsrecht des Betroffenen besteht im Widerspruchsrecht. Soweit der Betroffene der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten schriftlich widerspricht und darüber hinaus darlegen kann, dass die Verarbeitung seine besonderen persönlichen Interessen beeinträchtigt, darf nach § 25 Abs. 3 Satz 2 DSG M-V ein Umgang

mit den Daten nur erfolgen, wenn ein überwiegendes öffentliches Interesse gegeben ist. Das Ergebnis, ob dem Widerspruch stattgegeben wurde, ist dem Betroffenen in Schriftform mitzuteilen. Dem Umgang mit den Daten zur Gefahrenabwehr, Strafverfolgung und Steuerfahndung kann ausnahmsweise nicht widersprochen werden. Gem. § 25 Abs. 4 DSG M-V steht dem Betroffenen auch dann ein Widerspruchsrecht zu, wenn die Daten zum Zweck der Direktwerbung weitergegeben werden sollen; über diese Widerspruchsmöglichkeit muss die verantwortliche Stelle den Betroffenen ausdrücklich hinweisen.

3.1.8.7 Recht auf Schadenersatz

Entsteht dem Betroffenen ein Schaden, der aus einer unzulässigen oder unrichtigen automatisierten Verarbeitung seiner Daten beim Geoportal resultiert, so ist es verschuldensunabhängig nach § 27 DSG M-V zum Ersatz dieses Schadens verpflichtet. Das Gleiche gilt für eine nicht automatisierte Datenverarbeitung personenbezogener Daten, es sei denn das Geoportal kann nachweisen, dass es den Schaden nicht zu vertreten hat. Die Haftung ist auf die Höchstsumme von 125.000 Euro begrenzt und erfasst gleichermaßen die automatisierte wie die nichtautomatisierte Verarbeitung von personenbezogenen Daten.

3.1.8.8 Recht auf Anrufung des Landesdatenschutzbeauftragten

Aus § 26 DSG M-V ergibt sich das jedermann zustehende Recht, den Landesbeauftragten für Datenschutz zu kontaktieren, wenn die Annahme besteht, dass öffentliche Stellen gegen den Datenschutz verstoßen und dadurch seine Rechte verletzt wurden. Die Einhaltung des Dienstwegs ist für Beschäftigte des Geoportals, wenn sie solche Missbräuche erkannt haben und melden wollen, nicht notwendig; sie können direkt auf den Landesbeauftragten für Datenschutz zugehen.

3.2 Bereichsspezifische datenschutzrechtliche Vorschriften

Der Betreiber des Geoportals ist Diensteanbieter im Sinne des § 2 Nr. 1 TMG, da das Webportal zur Anzeige der digitalen Leitungsnetzdaten ein Telemediendienst darstellt. Gemäß § 1 Abs. 1 TMG ist der Anwendungsbereich des Telemediengesetzes in Bezug auf den Geoportalbetreiber eröffnet. Die Vorschriften des Telemediengesetzes sind im Verhältnis zu den allgemeinen Datenschutzvorschriften des Landesdatenschutzgesetzes spezieller, weshalb sie gem. § 2 Abs. 4 Satz 1 DSG M-V vorrangig Beachtung finden müssen, soweit der Anwendungsbereich des Telemediengesetzes reicht.

Die Bestimmungen des Telemediengesetzes über den Datenschutz sind in vollem Umfang zu beachten, da gemäß § 11 TMG ein Anbieter-Nutzer-Verhältnis zwischen dem Geoportal und seinen Nutzern vorliegt. Außerdem liegt bei dem angebotenen Dienst ein Telemedium vor, das gerade nicht überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht.

§ 12 TMG normiert die Grundsätze, die jeder Anbieter von Telemedien zu beachten hat. Zunächst ist das Erheben und Verwenden personenbezogener Daten der Nutzer zur Bereitstellung des Dienstes nur soweit erlaubt, wie das Telemediengesetz oder eine andere Rechtsvorschrift dies gestattet und sich dabei ausdrücklich auf Telemedien bezieht. Als eine Zulässigkeitsalternative ist die Einwilligung des Nutzers zu betrachten. Dasselbe gilt für die Verwen-

dung der personenbezogenen Daten des Nutzers, wenn sie für andere Zwecke als die Bereitstellung des Telemediendienstes eingesetzt werden sollen. Man spricht hier vom Gebot der Zweckbindung der Daten.

3.2.1 Anfallende Daten

Im Rahmen des Kommunikationsprozesses zwischen Geoportal und Nutzer, ggf. auch zusätzlich mit den Stellen, die die digitalen Geodaten bereitstellen, fallen verschiedene Daten an, die jeweils unterschiedlichen Kategorien zugeordnet werden können. Von Relevanz sind Bestands-, Nutzungs-, Abrechnungs- und Inhaltsdaten.

Inhaltsdaten im Rahmen des Kommunikationsvorgangs sind als solche Daten zu bezeichnen, die den eigentlichen Informationsgehalt der Übertragung darstellen. Sie dienen dazu, die im Rahmen des Teledienstes begründeten Leistungs- und Rechtsverhältnisse zu erfüllen.[27] Auf diese Art von Daten sind die Vorschriften des – im Verhältnis zum Telemediengesetz allgemeinen – Landesdatenschutzgesetzes anzuwenden. Zu diesen Daten gehören zum Beispiel die Daten des Antrags auf einen Schachtschein oder eine Leistungsnetzauskunft, die Daten in diesen beiden Dokumenten und die Daten zur Abrechnung der Kosten des Schachtscheins.

Was es im Zusammenhang mit den drei anderen Datenkategorien zu beachten gilt, ist nachfolgend dargestellt.

3.2.1.1 Bestandsdaten

Gemäß § 14 Abs. 1 TMG sind unter Bestandsdaten die personenbezogen Daten des Nutzers zu fassen, die für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses zur Erbringung des Telemediendienstes erforderlich sind.

Bestandsdaten sind somit Basisdaten, die zur Abwicklung des Vertragsverhältnisses für die Online-Portalnutzung benötigt werden. Im Zusammenhang mit dem Projekt TRUFFLE stellen Bestandsdaten insbesondere nachfolgende nutzerbezogene Informationen dar:

- Vor- und Zuname,
- Anschrift,
- Telefonnummer,
- E-Mail-Adresse und
- Zugangspasswort.[28]

Der Datenumgang mit den Bestandsdaten innerhalb der das Geoportal betreibenden Stelle hat sich am Grundsatz der Datensparsamkeit zu orientieren. Konkret bedeutet dies, dass nur die Erhebung und Verwendung der personenbezogenen Daten des Nutzers erforderlich ist, welche für die Begründung, Gestaltung oder Änderung des Telemediendienstevertrags unerlässlich ist.[29] Darüber hinaus gilt die in § 12 Abs. 1 TMG manifestierte Zweckbindung, die den Datenumgang in diesem Zusammenhang nur in enger Verbindung zum Vertragsverhältnis zulässt.[30]

[27] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 12 TMG Rn. 4.
[28] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 14 TMG Rn. 3.
[29] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 14 TMG Rn. 4.
[30] *Gitter*, Softwareagenten im elektronischen Geschäftsverkehr, 2007, 310.

3.2.1.2 Nutzungsdaten

Zu Abrechnungszwecken und, falls dies für die Inanspruchnahme des Telemediendienstes erforderlich ist, zur Bereitstellung des Dienstes darf der Diensteanbieter gem. § 15 Abs. 1 TMG personenbezogene Daten des Nutzers erheben und verwenden; diese Daten sind als Nutzungsdaten einzuordnen.

Unter sie fallen hauptsächlich

- Kennzeichen, die zur Identifikation des Nutzers dienen,
- Zeitpunkt des Beginns und der Beendigung der Nutzung sowie Angaben über deren Umfang und
- Informationen über die in Anspruch genommenen Dienste beim Geoportal.

3.2.1.3 Abrechnungsdaten

Abrechnungsdaten sind nach § 15 Abs. 4 TMG solche Nutzungsdaten, die für die Abrechnung der in Anspruch genommen Dienste durch den Nutzer notwendig sind. Hierzu würden Kostendaten dann gehören, wenn für die telemediale Beantragung eigene medienspezifische Kosten erhoben würden. Da dies nicht beabsichtigt ist, spielt diese Datenkategorie für das Geodatenportal keine große Rolle.

3.2.2 Pflichten des Diensteanbieters

In § 13 TMG werden dem Telemediendiensteanbieter verschiedene Pflichten bezüglich des Datenschutzes auferlegt, die das Geoportal im Rahmen der Ausübung seiner Tätigkeit zu erfüllen hat.

Anmerkung: Die Informationspflicht aus § 5 TMG fällt zwar nicht in den Bereich der datenschutzrechtlichen Verpflichtungen, stellt jedoch eine allgemeine Notwendigkeit beim Anbieten von Telemedien dar und ist deshalb mit in den Katalog der Pflichten aufgenommen.

3.2.2.1 Allgemeine Informationspflichten

§ 5 TMG enthält allgemeine Informationspflichten (sog. Impressumspflicht[31]), die insbesondere dem Verbraucherschutz dienen. Betroffene sollen von der Stelle, die ihre Daten erhebt, verarbeitet und nutzt, Kenntnis erlangen und ggf. ihre Rechte gegenüber dieser Stelle durchsetzen können.[32] So müssen in erster Linie Name, Anschrift und Angaben zur schnellen elektronischen Kontaktaufnahme im Impressum enthalten sein. Das Impressum ist leicht erkennbar, unmittelbar erreichbar auf der Webseite zu platzieren und muss ständig verfügbar sein. Weitere notwendige Angaben sind dem § 5 TMG zu entnehmen.

Die besonderen – und im Vergleich zu § 5 TMG weitergehenden – Informationspflichten bei kommerzieller Kommunikation aus § 6 TMG gilt es im Zusammenhang mit dem Geoportal

[31] Das Bundesministerium der Justiz stellt eine Orientierungshilfe bereit, die zur rechtskonformen Umsetzung der Impressumspflicht dienen soll (Leitfaden abrufbar unter: http://www.bmj.de/musterimpressum).
[32] *Micklitz*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, TMG, 2008, § 5 Rn. 2.

nicht zu beachten, da seine Tätigkeit jedenfalls kein Handeln im geschäftlichen Verkehr zu Wettbewerbszwecken darstellt.[33]

3.2.2.2 Unterrichtungspflicht

Dem Anbieter des Geoportaldienstes obliegt gem. § 13 Abs. 1 TMG die Verpflichtung, den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke des Umgangs mit seinen personenbezogenen Daten in verständlicher Form aufzuklären. Wurde der Nutzer bereits vor dem Nutzungsvorgang darüber in Kenntnis gesetzt, ist eine diesbezügliche Information zu Beginn der Nutzung entbehrlich. Kommt ein automatisiertes Verfahren zur Anwendung, das die spätere Identifizierung des Nutzers ermöglicht und zur Vorbereitung einer personenbezogenen Erhebung oder Verwendung von Daten dient, also Cookies oder ähnliche Identifizierungsmechanismen eingesetzt werden,[34] muss eine diesbezügliche Aufklärung des Nutzers zu Beginn des Vorgangs erfolgen.

Darüber hinaus gilt es zu beachten, dass die jederzeitige Abrufbarkeit der Inhalte der Unterrichtung sichergestellt ist. Dieser Forderung kann das Geoportal genügen, indem es die entsprechenden Hinweise beispielsweise direkt auf der Webseite anbringt oder mittels eines Links auf sie aufmerksam macht.[35]

3.2.2.3 Technische und organisatorische Vorkehrungen

Das Geoportal ist gem. § 13 Abs. 4 TMG durch technische und organisatorische Maßnahmen so zu gestalten, dass bestimmte Voraussetzungen erfüllt sind. So muss

- der jederzeitige Nutzungsabbruch der Dienste durch den Nutzer möglich sein,
- die sofortige Löschung bzw. Sperrung der personenbezogenen Daten nach Nutzungsende erfolgen,
- der Nutzer den Dienst vertraulich in Anspruch nehmen können,
- eine getrennte Nutzungsmöglichkeit der personenbezogenen Daten eines Nutzers bei verschiedenen Telemedien gegeben sein,
- sichergestellt werden, dass die Zusammenführung von Daten eines Nutzers über die Inanspruchnahme verschiedener Telemediendienste desselben Diensteanbieters ausschließlich zu Abrechnungszwecken möglich ist,
- die Zusammenführung von Nutzungsprofilen mit den Trägern der Pseudonyme verhindert werden.

Sämtliche in Abs. 4 enthaltenen Maßnahmen dienen dem Grundsatz des Systemdatenschutzes. Technische Systeme werden hiernach so gestaltet, dass die Datenverarbeitung nur noch entsprechend der gesetzlichen Ermächtigung möglich ist. Ferner dürfen nur noch solche Daten verarbeitet werden können, für die eine Verarbeitungsbefugnis besteht.[36]

[33] *Micklitz*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, TMG, 2008, § 6 Rn. 16.
[34] S. *Roßnagel/Banzhaf/Grimm*, Datenschutz im Electronic Commerce, 2003, 71 ff.
[35] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, TMG, 2008, § 13 Rn. 5.
[36] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, TMG, 2008, § 13 Rn. 8.

3.2.2.4 Bereitstellung einer anonymen Nutzungsmöglichkeit

Im Grundsatz hat der Diensteanbieter die Inanspruchnahme seines Diensteangebots sowie dessen Bezahlung gem. § 13 Abs. 6 TMG anonym oder pseudonym zu ermöglichen. Einschränkende Bedingung dafür ist, dass es dem Betreiber technisch möglich und zumutbar ist. Falls die Möglichkeit der anonymen oder pseudonymen Nutzung des Geoportals existiert, hat eine diesbezügliche Information des Nutzers zu erfolgen.

Anonymisieren ist gem. § 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". Bei anonymisierten Daten handelt es sich nicht mehr um personenbezogene Daten, da die Person unbekannt ist oder es nach praktischer Lebenserfahrung ausscheidet, dass ihre Identität aufgedeckt wird.[37] Im Rahmen der Dienstenutzung (Prüfung des berechtigten Interesses, Zuweisung einer Nutzerrolle etc.) und -abrechnung (Bezahlung der kostenpflichtigen Auskünfte) ist es jedoch erforderlich, dass sich der Nutzer einmalig beim Geoportal registriert und sich bei jedem weiteren Zugriff gegenüber dem Geoportal authentifiziert. Dies hat zur Folge, dass das Anbieten einer anonymen Nutzungsmöglichkeit des Geoportals ausscheidet.

Unter Pseudonymisieren hingegen ist gem. § 3 Abs. 6a BDSG „das Ersetzen des Namens und anderer Identifikationsmerkmale durch Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren" zu verstehen. Grundsätzlich erfolgt hierbei ein personenbezogenes Verarbeiten von Daten, wobei jedoch nur derjenige, der die Zuordnungsregel kennt, den Personenbezug herzustellen vermag. Eine Möglichkeit, dem Nutzer pseudonymes Handeln zu eröffnen, besteht in der freien Wählbarkeit von beliebigen Benutzernamen.[38] Agieren unter Pseudonym ermöglicht die Identifizierung von Vertragspartnern und Trägern von Berechtigungen, wie sie im Rahmen von TRUFFLE notwendig ist. Es existieren generell drei Arten von Pseudonymen, wobei im Zusammenhang mit dem Geoportal nur eine Variante verwendet werden kann: Sie besteht darin, dass das Geoportal die Zuordnungsregel Nutzer zu Pseudonym kennt, das Pseudonym folglich nicht gegenüber dem Portal, sondern gegenüber Dritten schützt.[39] Soweit das Portal, das die Aufdeckungsregeln kennt, allerdings der einzige Kontakt des Nutzers unter dem Decknamen ist, hat die Wahl eines Decknamens keine datenschutzrechtliche Schutzwirkung.

3.2.2.5 Auskunftspflicht

Der Diensteanbieter ist gem. § 13 Abs. 7 TMG verpflichtet, dem Nutzer Auskunft über zu seiner Person oder seinem Pseudonym gespeicherte Daten zu erteilen, falls der Nutzer Auskunft darüber ersucht. Die Auskunft hat sich an den Maßstäben des § 34 BDSG zu orientieren. Dieser Informationspflicht kann das Geoportal auch mit elektronischen Auskünften nachkommen.

Die Verpflichtung des Diensteanbieters zur Auskunft dient der Transparenz; ohne die Vorschrift des § 13 Abs. 7 TMG könnte der Nutzer seine Rechte, beispielsweise auf Sperrung,

[37] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, TMG, 2008, § 13 Rn. 11.
[38] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, TMG, 2008, § 13 Rn. 15.
[39] *Roßnagel/Scholz*, MMR 2000, 721 (724 ff.).

Berichtigung und Löschung, überhaupt nicht wahrnehmen, da er nicht weiß, welche Daten über ihn gespeichert werden.[40]

[40] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, TMG, 2008, § 13 Rn. 16.

4 Juristische Betrachtung der Prozesse

4.1 Verhältnis zwischen Geoportal und datenliefernden Stellen

4.1.1 Umgang mit unterschiedlichen Nutzungsbestimmungen

In Bezug auf den Umgang mit unterschiedlichen Nutzungsbestimmungen der Datenlieferanten – etwa was die Gültigkeitsdauer der erteilten Auskünfte anbelangt –, die dem Geoportal ihre jeweiligen fachspezifischen Geodaten zur Verfügung stellen, existieren grundsätzlich verschiedene Möglichkeiten:

- Bei weitgehend homogenen Klauseln der Datenlieferanten können die Nutzungsbestimmungen des Geoportals an die jeweiligen Klauseln auf niedrigstem oder höchstem Niveau angepasst werden. An einem Beispiel lässt sich eine solche Vorgehensweise veranschaulichen: Wenn „Datenlieferant“ 1 eine ein-, „Datenlieferant“ 2 eine zwei- und „Datenlieferant“ 3 eine dreimonatige Gültigkeit ihrer jeweiligen Auskünfte garantieren, so kann das Geoportal unproblematisch generell – für sämtliche Daten – eine einmonatige Gültigkeitsdauer zusichern.
- Insbesondere bei stark differierenden Klauseln der einzelnen Datenlieferanten bietet es sich an, separate – nur im Zusammenhang mit dem Geoportal gültige – Nutzungsbestimmungen zu entwickeln, die von sämtlichen Datenlieferanten zu akzeptieren sind. Ein solches Vorgehen diente der starken Vereinfachung, da sich damit eine Homogenisierung der Nutzungsbestimmungen im Verhältnis zwischen Geoportal und Datenlieferanten erreichen lässt.
- Auch können für die unterschiedlichen Datenbestände (Strom, Gas etc.) jeweils eigene Nutzungsbestimmungen vorgesehen werden. Die Nutzungsbestimmungen des Geoportals müssten in diesem Fall die spezifischen Bedingungen für die einzelnen Datenbestände enthalten. Bei dieser Variante ist die Haftung für miteinander verschnittene Daten innerhalb einer Karte ausgeschlossen. Eine Haftung sollte nur für Einzelauskünfte (Strom, Gas etc. jeweils separat) übernommen werden und für diese die spezifischen Nutzungsbestimmungen der einzelnen Datenlieferanten gelten.

4.1.2 Schutzrechte in Bezug auf Geoinformationen

Die spezifischen Geofachdaten, welche von den verschiedenen Datenlieferanten an das Geoportal übermittelt werden, unterliegen gesetzlichen Schutzrechten. Allgemein resultieren solchen Schutzrechte aus dem Urheberrechtsgesetz, dem Gesetz gegen unlauteren Wettbewerb sowie aus den Vermessungsgesetzen der Länder.

Je nach Art der Geofachdaten (analog, digital etc.) kann ihnen Schutz aus

- § 2 Abs. 1 Nr. 7 UrhG
- § 4 Abs. 2 UrhG
- § 72 UrhG
- § 87a ff. UrhG

zukommen.

Aus diesem Grund müssen dem Geoportal sog. Nutzungsrechte eingeräumt werden, in deren Rahmen das Geoportal die Befugnis erhält, die Daten zu verarbeiten. Die Verschneidung der

Daten mit anderen Daten eines weiteren Datenlieferanten, um mehrere Schichten zu erzeugen, stellt eine solche Datenverarbeitung dar. Das mit dem Geoportal vereinbarte Nutzungsrecht muss insbesondere das Recht für die Portalnutzer enthalten, die ihnen erteilten Auskünfte für einzelne Vorhaben (z. B. Planung einer Baumaßnahme) nutzen zu können. Einschränken lassen sich die Nutzungsrechte für Portalnutzer insbesondere durch die Nutzungsbestimmungen des Geoportals.[41]

Nach dem Gesetz gegen unlauteren Wettbewerb sind unlautere geschäftliche Handlungen zur Erzielung von Wettbewerbsvorteilen unzulässig. Eine solche verbotene Vorgehensweise zum Ausbau der eigenen Wettbewerbskraft kann darin bestehen, dass Geodaten ohne Genehmigung genutzt werden. Geoinformationen können dem Leistungsschutz gem. § 1 UWG unterliegen.

§ 34 Abs. 1 GeoVermG M-V legt fest, dass Geobasisdaten nur für den Zweck genutzt werden dürfen, für den sie bereitgestellt wurden. Beabsichtigte Nutzungen dieser Daten bedürfen der Zustimmung der zuständigen Vermessungs- und Geoinformationsbehörde. Gem. Abs. 2 besteht jedoch die Möglichkeit, ein nicht ausschließliches Rechts zur Nutzung von Geobasisdaten einzuräumen. Das GeoVermG M-V enthält in § 15 Abs. 4 darüber hinaus einen Verweis auf das Urheberrechtsgesetz.

4.2 Verhältnis zwischen Geoportal und Nutzer

4.2.1 Zulässigkeit des Datenabrufs aus dem Portal

Da die Daten, die der Nutzer aus dem Portal abruft, im Regelfall personenbezogene Daten beinhalten, ist der Abruf nach der Spezialvorschrift des künftigen § 15 Abs. 2 Satz 2 Nr. 1 GeoVermG M-V einzuschränken, wenn dadurch personenbezogene Daten offenbart würden und damit eine Beeinträchtigung von schutzwürdigen Interessen der Betroffenen einherginge, es sei denn von diesen liegt eine diesbezügliche Einwilligung vor. Diese Vorschrift dient dem Schutz des informationellen Selbstbestimmungsrechts von Betroffenen.[42]

Ob der Zugang zu personenbezogenen Geodaten – ohne den generell unpraktikablen Umweg über die Einwilligung – eröffnet werden kann, hängt maßgeblich davon ab, ob schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Es handelt sich hierbei um eine Abwägungsfrage, in welcher der Informationsanspruch des Antragstellers dem informationellen Selbstbestimmungsrecht des Betroffenen gegenüberzustellen ist.[43]

Leitungen, die unter einem Grundstück verlegt sind, besitzen im Regelfall keine Aussagekraft im Hinblick auf die Persönlichkeit des Grundstückseigentümers. Allenfalls sind dann Rückschlüsse auf die finanzielle Situation des Grundstückseigentümers denkbar, wenn am Leitungsbestand erkennbar ist, dass sich beispielsweise Swimming- oder Whirlpools auf dem Grundstück befinden. Die datenschutzrechtliche Schutzwürdigkeit von Informationen über den Leitungsbestand eines Grundstücks ist allgemein als niedrig einzustufen, da sie keine empfindlichen Daten darstellen, deren Bekanntgabe an Berechtigte zur Verletzung des Persönlichkeitsrechts von Betroffenen führte. Andererseits kann ein Schaden am Versorgungsnetz derart gravierende negative ökologische, ökonomische und soziale Auswirkungen haben, dass der Vermeidung eines solchen im Rahmen einer Rechtsgüterabwägung der höhere Rang

[41] S. zum Urheberrecht auch 4.2.3.1.
[42] LT M-V Drs. 5/3476, 62.
[43] LT M-V Drs. 5/3476, 62.

beizumessen ist. Ein dazu befugter Antragsteller hat das berechtigte Interesse an der Kenntnis der Leitungsinformationen, da er nur mit Hilfe dieser Daten erhebliche Umweltschäden vermeiden und der eigenen Haftung entgehen kann.

Die vom Geoportal des ZVG intendierte vereinfachte Abrufbarkeit von grundstücksbezogenen Auskünften über den Leitungsbestand ist in Bezug auf Privatpersonen aus Sicht des Datenschutzes ferner deshalb unproblematisch, weil der Antragsteller nur solche Leitungsdaten abrufen kann, die ihn selbst betreffen; es sind keine personenbezogenen Daten anderer involviert.

Was die verschiedenen Stellen – wie der ZVG selbst, das Straßenbauamt, die Bauunternehmen und Planungsbüros – anbelangt, die aus öffentlichen oder beruflichen Interessen auf die Daten zugreifen, so kann diesen ein berechtigtes Interesse am Zugang zu den Leitungsnetzdaten privater Grundstücke und öffentlicher Flächen qua ihrer Amtsaufgabe oder ihres beruflichen Tätigkeitsfelds unterstellt werden. Hinsichtlich welcher spezifischen Geoinformationen ein überwiegendes Interesse für den Zugang der jeweiligen Stelle vorliegt, wird im Rahmen der Registrierung beim Geoportal durch einen Sachbearbeiter des ZVG geprüft. Dieser Mitarbeiter weist der jeweiligen Stelle eine definierte Nutzerrolle zu, die bestimmte Zugangsrechte umfasst. Die Rechtevergabe ist abhängig vom Aufgabengebiet der Stelle und auf räumlicher und inhaltlicher Ebene eingeschränkt. Weisen besondere Umstände auf eine Beeinträchtigung von schutzwürdigen Interessen der Betroffenen hin, ist der Zugang so zu beschränken, dass die Beeinträchtigung ausgeschlossen wird.

Aufgrund dieser generellen Abwägung ist es beim Zugriff überprüfter und zugelassener Nutzer im jeweiligen Einzelfall ausreichend, wenn die Zugriffsberechtigung geprüft wird. Geben zusätzliche Erkenntnisse Hinweise auf eine Beeinträchtigung, ist die Zugriffsberechtigung im Einzelfall oder ganz zu entziehen. Zum Schutz der informationellen Selbstbestimmung erscheinen Stichprobenkontrollen hinsichtlich einer Beeinträchtigung im Einzelfall ausreichend.

4.2.2 Zugang zum System

Da die vom Geoportal bereitgestellten Informationen insbesondere vor unberechtigtem Zugriff geschützt werden müssen, ist die eindeutige Zuordnung einer natürlichen Person zu ihrem Nutzerkonto sicherzustellen.

4.2.2.1 Registrierung des Nutzers

Damit das Geoportal prüfen kann, ob ein berechtigtes Interesse des jeweiligen Nutzers in Bezug auf ein bestimmtes geografisches Gebiet gegeben ist, muss auf dieser Grundlage die Zuweisung einer Nutzerrolle mit bestimmten Rechten erfolgen. Zu diesem Zweck und zur Abrechnung der in Anspruch genommenen kostenpflichtigen Dienste ist vor der erstmaligen Nutzung der Dienste eine Registrierung des Nutzers mit seinen persönlichen Daten vorzunehmen. Die dabei erhobenen personenbezogenen Daten des Nutzers stellen Bestandsdaten gem. § 14 Abs. 1 TMG dar. Sie dienen der Begründung, der inhaltlichen Ausgestaltung oder der Änderung des Vertragsverhältnisses.

Sofern der Antragsteller seinen Antrag nicht in den Geschäftsräumen des Geoportals stellt, sind geeignete Formen der sicheren Identifizierung des Antragstellers zu nutzen:

4.2.2.1.1 Registrierung mittels Postident-Verfahren

Das sog. Postident-Verfahren[44], das die Deutsche Post AG zur eindeutigen Identifikation von natürlichen Personen anbietet, kann als sichere Methode zur Nutzerregistrierung eingesetzt werden. Im Rahmen dieses Verfahrens werden sämtliche Daten des Ausweispapiers (Personalausweis oder Reisepass) erfasst sowie durch Unterschrift des Ausweisinhabers bestätigt. Dies erfolgt in einer Postfiliale oder beim Nutzer mittels eines Erfüllungsgehilfen der Deutschen Post AG.[45] Die Identität des (zukünftigen) Nutzers gilt somit als eindeutig festgestellt und kann von ihm nicht mehr bestritten werden.

4.2.2.1.2 Registrierung mittels Elektronischem Personalausweis

Mit der Einführung des Elektronischen Personalausweises im November 2010 eröffnen sich neue Möglichkeiten zur elektronischen Identifikation; insofern gilt ein Grundproblem des E-Commerce und E-Government als künftig gelöst. Mit stetiger Zunahme von online abgewickelten Geschäftsprozessen wächst das Bedürfnis nach Rechtssicherheit. Eine zwingende Voraussetzung dazu ist, dass die Kommunikationspartner bekannt sind.[46]

Zukünftig können sich Ausweisinhaber im Internet elektronisch ausweisen, da sämtliche Daten, die heutzutage optisch auslesbar sind, künftig in einem Ausweis-Chip gespeichert werden. Der Ausweisinhaber vermag sich somit im Internet elektronisch auszuweisen, da der elektronische Personalausweis über die Funktion des elektronischen Identitätsnachweises verfügt. Verschiedene internetbezogene Prozesse, wie Login und Altersnachweis, lassen sich effizient und zeitsparend umsetzen.[47]

Der Prozess des elektronischen Identitätsnachweises wird nur in Gang gesetzt, wenn der Ausweisinhaber seine PIN eingibt und der Diensteanbieter ein Berechtigungszertifikat, das ihn zur Durchführung des Identitätsnachweises berechtigt, an den Ausweisinhaber zurückgibt. Der Geoportalbetreiber muss folglich über ein solches Zertifikat verfügen; es wird bei Vorliegen bestimmter Voraussetzungen gem. § 21 Abs. 3 Satz 1 PAuswG zeitlich befristet ausgestellt.[48]

Die Nutzung des elektronischen Identitätsnachweises ist auch im Rahmen des Geoportals sinnvoll, soweit eine eindeutige Identifizierung beim Erstkontakt oder bei der Wiedererkennung (Authentifizierung bei jeder Nutzung) notwendig ist.

4.2.2.1.3 Registrierung mittels Bürgerportalen

Grundsätzlich besteht die Möglichkeit, die Identifizierungsdienstleistung („De-Ident“) der von Bürgerportalen bereitgestellten „De-Mail“ zur Registrierung des Nutzers beim Geoportal einzusetzen. Mit dieser Funktion können Diensteanbieter, wie das Geoportal, zuverlässig und unter Einhaltung des Datenschutzrechts Identitätsdaten des Bürgerportal-Nutzers aufneh-

[44] S. insbesondere zu zivilrechtlichen Aspekten von Postident ausführlich *Möller*, NJW 2005, 1605 ff.
[45] § 1 Abs. 1 Nr. 4 AGB PostIdent-Service.
[46] *Hornung*, WIK 2009/5, 29, 31; *Roßnagel/Hornung/Schnabel*, DuD 2008, 168 ff.
[47] S. http://www.bmi.bund.de.
[48] *Roßnagel/Hornung*, DÖV 2009, 301 ff.; *Hornung*, WIK 2009/5, 29, 31.

men.[49] Die Registrierung bei De-Mail erfolgt mit Personalausweis oder Pass, die Authentifizierung bei der Nutzung erfolgt ebenfalls in sicherer Weise durch zwei Sicherungsmittel. Elektronische Nachrichten, die mittels De-Mail-Dienst verschickt werden, lassen sich für rechtsverbindliche Vorgänge nutzen.[50]

Ein eindeutiger Vorzug der Funktion De-Ident ist die medienbruchfreie zuverlässige Registrierungsmöglichkeit bei Diensteanbietern, die ein Benutzerkonto erfordern. Diesen Bürgerportaldienst können nicht nur natürliche Personen, sondern auch juristische Personen des privaten und öffentlichen Rechts nutzen.[51]

4.2.2.2 Prüfung des berechtigten Interesses und Zuweisung der Nutzerrolle

Den unterschiedlichen Nutzerkategorien, die sich beispielsweise aus

- Planungsbüros,
- Privatpersonen,
- Versorgungsunternehmen und
- dem ZVG selbst

zusammensetzen, sollen jeweils verschiedene Rollen zugewiesen werden, die spezifische Rechte beinhalten. Die jeder einzelnen Rolle zugeteilten Nutzungsrechte unterscheiden sich sowohl in funktionaler als auch inhaltlicher Hinsicht: So stehen einer Privatperson nur diejenigen Informationen zur Verfügung, die im Regelfall zur Beurteilung eines Bauvorhabens ausreichen, während Mitarbeitern des ZVG Zugriff auf alle Datenbestände haben, die sie zur Erledigung ihrer Aufgaben benötigen. Es wurde eine rollenspezifische Beschränkung auf Ebene der darstellbaren Koordinatenbereiche und Layer (bspw. Gasleitungen, Straßennetz oder Gewässer) implementiert. Die Differenzierung nach verschiedenen Rollen mit zugehörigen Rechten ist aus Gründen des Datenschutzes unabdingbar.

Da keine automatisierte und medienbruchfreie Identifizierung des jeweiligen Nutzers stattfindet, an die sich darüber hinaus eine automatische Rollenzuweisung anschließt, liegt diesbezüglich keine automatisierte Einzelentscheidung i. S. d. § 12 DSG M-V vor. Diese Registrierung und Zuordnung soll vielmehr durch einen Sachbearbeiter vorgenommen werden, der in jedem Einzelfall die Voraussetzungen für den Zugang zum Geoportal prüft.

Auch in der Abfrage des Nutzernamens mit zugehörigem Passwort im Rahmen des Anmeldevorgangs beim Geoportal ist keine automatisierte Einzelentscheidung zu sehen: Die Zuweisung der jeweiligen Nutzerrolle mit zugehörigen Rechten erfolgt durch einen Mitarbeiter des ZVG bei der Registrierung des Nutzers. Meldet sich der Nutzer anschließend beim Geoportal an, erfolgt lediglich die programmtechnische Umsetzung der bereits festgelegten Zuordnungen; das System selbst trifft dabei keinerlei Entscheidungen.

[49] *Bundesministerium des Innern*, Bürgerportale, 14 (abrufbar unter: http://www.cio.bund.de/cae/servlet/contentblob/78162/publicationFile/40451/ueberblick_vo_download.pdf).
[50] *Roßnagel/Hornung/Knopp/Wilke*, De-Mail und Bürgerportale – Eine Infrastruktur für Kommunikationssicherheit, DuD 2009, 728 ff.; *Höfling*, Staat & IT, 12/2008, 26 (27).
[51] *Bundesministerium des Innern*, Bürgerportale, 2 ff. (abrufbar unter: http://www.cio.bund.de/cae/servlet/contentblob/78162/publicationFile/40451/ueberblick_vo_download.pdf).

4.2.3 Nutzung des Systems

4.2.3.1 Urheberrechtlicher Schutz

Die vom Geoportal bereitgestellte Bestandsauskunft im pdf-Dateiformat enthält neben Geobasisdaten, die lediglich eine Grundkarte darstellen, spezifische Infrastrukturdaten bezüglich Art und Lage erdverlegter Leitungen. Gem. § 2 Abs. 1 Nr. 7 UrhG können geschützte Werke u. a. Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen sein. Voraussetzung für das Vorliegen des urheberrechtlichen Schutzes ist, dass die Darstellung eine eigene schöpferische Leistung enthält. Eine herkömmliche Landkarte ist gegen die Übernahme individueller Gestaltungsmerkmale geschützt, nicht aber in Bezug auf die topografische Grundlage, die bei sämtlichen Karten über dasselbe Gebiet identisch ist.[52] Die Abbildung des Leitungsnetzes auf der durch die Natur vorgegebene Grundkarte ist als ein solches individuelles Gestaltungsmerkmal, das eine bestimmte geistige Schöpfungshöhe darstellt, zu sehen. Die Anforderungen an die notwendige Individualität im Zusammenhang mit kartografischen Abbildungen sind relativ gering, da in diesem Werkbereich aufgrund der Sachzwänge ein sehr geringer eigener Gestaltungsspielraum vorliegt.[53] Die konkrete Formgebung einer kartografischen Darstellung ist vom urheberrechtlichen Schutz aus § 2 Abs. 1 Nr. 7 UrhG gedeckt. Die bloßen Vermessungsdaten, die das Ergebnis wissenschaftlicher Ermittlung und Berechnung sind, und auf deren Grundlage die Abbildung der Grundkarte überhaupt möglich ist, fallen demgegenüber nicht unter den urheberrechtlichen Schutz.[54] Insgesamt ist der in der pdf-Datei abgebildete Kartenausschnitt, der das Leitungsnetz enthält, jedoch urheberrechtlich geschützt.

Dem Urheber eines Werkes steht nach § 15 Abs. 1 UrhG insbesondere das alleinige Recht zu, es in körperlicher Form zu verwerten. Für die geforderte körperliche Festlegung ist es ausreichend, das Werk mittelbar der menschlichen Sinneswahrnehmung zugänglich zu machen. Diese mittelbare Zugänglichmachung wird durch Speicherung der digitalen Geodaten auf einem Speichermedium verwirklicht.[55] Die Verwertung des Werks kann sich in der Vervielfältigung nach § 16 UrhG, der Verbreitung nach § 17 UrhG und der Ausstellung nach § 18 UrhG vollziehen. Ebenso steht dem Urheber nach § 19a UrhG das alleinige Recht zu, sein Werk elektronisch der Öffentlichkeit zugänglich zu machen.

Von zentraler Bedeutung ist die Vorschrift des § 31 UrhG, der die Einräumung von Nutzungsrechten reglementiert. § 31 Abs. 1 UrhG legt fest, dass der Urheber eines Werkes anderen verschiedene Nutzungsrechte einräumen kann. Die Nutzungsrechte können dabei als einfache oder ausschließliche Rechte und mit Restriktionen in räumlicher, zeitlicher oder inhaltlicher Hinsicht gewährt werden. In der Überlassung der Bestandsauskunft – in Form einer Datei im pdf-Format – beim Nutzer zu dessen Information über das Leitungsnetz ist die Einräumung eines solchen Nutzungsrechts zu sehen. Beschränkungen des Nutzungsrechts der digitalen Bestandsauskünfte kommen in den „Nutzungsbedingungen für übergebene digitale Bestandspläne“ in den Ziffern 2 bis 5 zum Ausdruck. So enthält etwa Ziffer 5 eine zeitliche Beschränkung des Nutzungsrechts, indem der Auftragnehmer dazu verpflichtet wird, die übermittelten Daten nach Durchführung des Auftrags zu löschen.

[52] *Bullinger*, in: Wandtke/Bullinger (Hrsg.), Urheberrecht, 3. Aufl. 2009, UrhG, § 2 Rn. 139; *Hertin*, GRUR 2004, 646 (647).
[53] *Bullinger*, in: Wandtke/Bullinger (Hrsg.), Urheberrecht, 3. Aufl. 2009, UrhG, § 2 Rn. 139.
[54] *Hertin*, GRUR 2004, 646 (652); *Schulze*, in: Dreier/Schulze, UrhG, 3. Aufl. 2008, § 2 Rn. 236.
[55] *Heerma*, in: Wandtke/Bullinger (Hrsg.), Urheberrecht, 3. Aufl. 2009, UrhG, § 15 Rn. 8.

Falls etwa Missbrauchsfälle im Zusammenhang mit den digitalen Bestandsplänen des Zweckverbandes bekannt werden, kann es unter Umständen notwendig sein, den Urheberschaftsnachweis zu erbringen. In einigen Fällen lassen sich eigene Rechtspositionen ohne diesen Nachweis nicht durchsetzen. Damit der Nachweis gelingt, muss die Datei ihren tatsächlichen Urheber erkennen lassen. Dabei ist es nicht notwendig – und in den meisten Fällen auch nicht sinnvoll –, dass beispielsweise das Firmenlogo optisch erkennbar in das Bild integriert wird. Das Problem solcher wahrnehmbaren Informationen besteht darin, dass sie relativ einfach entfernt werden können, etwa durch Abschneiden des Objektbereichs. Deshalb eignet sich vielmehr ein Verfahren, mit dem sich versteckte Informationen mit dem Dateimaterial „verweben" lassen. Die Löschung der verborgenen Botschaft ist grundsätzlich nicht möglich, ohne das Datenmaterial selbst zu beschädigen; somit sind Manipulationen erkennbar. Das genannte Verfahren besteht im Einbringen digitaler Wasserzeichen, einer Form der Steganographie. Die digitalen Wasserzeichen ermöglichen es, nicht wahrnehmbare Muster oder textuelle Nachrichten in unterschiedliches Dateimaterial (etwa Bild, Video und Audio) – auch unter Verwendung von Verschlüsselung – einzubringen. Es sollten dabei möglichst robuste Wasserzeichen eingesetzt werden, die sich auch trotz Komprimierungen und Formatkonvertierungen beständig halten.[56] Digitale Wasserzeichen eignen sich zwar nicht zum Unterbinden der unrechtmäßigen Weitergabe von digitalem Datenmaterial, mit ihrer Hilfe lassen sich jedoch unzweifelhaft die Urheberschaft von Daten und damit auch deren potenzieller Missbrauch nachweisen.[57]

4.2.3.2 Einbeziehung der „Nutzungsbedingungen für übergebene digitale Bestandspläne"

Gem. § 305 Abs. 1 Satz 1 BGB handelt es sich bei für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrags stellt, um sog. Allgemeine Geschäftsbedingungen (AGB). Die „Nutzungsbedingungen für übergebene digitale Bestandspläne" erfüllen diese Voraussetzungen, sodass die Bedingungen anhand der Vorschriften für die Gestaltung rechtsgeschäftlicher Schuldverhältnisse durch allgemeine Geschäftsbedingungen des Bürgerlichen Gesetzbuches zu beurteilen sind.

Auch wenn der Zweckverband, der das Portal betreibt, eine öffentlich-rechtliche Körperschaft ist, wird das Verhältnis zu den Nutzern nach privatrechtlichen Grundsätzen zu bewerten sein. Das Portal übt keine Hoheitsgewalt aus und das Verhältnis zwischen Portal und Nutzern entspricht nicht einem hoheitlichen Über- und Unterordnungsverhältnis. Vielmehr bietet das Portal an, Geodaten über Infrastrukturen von Versorgungsunternehmen berechtigten Nutzern zur Verfügung zu stellen. Diese Tätigkeit ist mit keiner Kontrolle, Bewertung und Ermächtigung der privaten Nutzer verbunden, sondern entspricht einem gleichberechtigten Austauschverhältnis. Daher kann das Portal Allgemeine Geschäftsbedingungen zur Regulierung dieser Austauschbeziehungen verwenden.

Gegenwärtig werden dem Nutzer die Nutzungsbedingungen zugesandt. Er muss sie unterschreiben und diese Erklärung per Telefax an den Zweckverband übermitteln. Damit bringt der Nutzer explizit zum Ausdruck, dass er die Nutzungsbedingungen akzeptiert und die Bestandsauskunft zu den vorgesehenen Konditionen erhalten will. Eine solch aufwändige Vorgehensweise ist äußerst unpraktisch und auch nicht notwendig: Gem. § 305 Abs. 2 BGB reicht es für das wirksame Einbeziehen solcher vorformulierten Geschäftsbedingungen völlig

[56] *Dittmann/Steinmetz*, Informatik Spektrum, 2/2000, 47 ff.
[57] *Arnold/Funk/Busch*, Technische Schutzmaßnahmen multimedialer Daten (abrufbar unter: http://www.igd.fraunhofer.de/igd-a8/syscop/Publications/Arnold00b.pdf).

aus, wenn der Verwender – also der Zweckverband – den Nutzer des Geoportals bei Vertragsschluss ausdrücklich auf die AGB hinweist und ihm eine zumutbare Möglichkeit einräumt, vom Inhalt der Geschäftsbedingungen Kenntnis nehmen zu können. Eine weitere Wirksamkeitsvoraussetzung zur Einbeziehung von AGB stellt das Einverständnis des Nutzers dar. Aus Gründen der Vollständigkeit wird erwähnt, dass auf den ausdrücklichen Hinweis auf die AGB ausnahmsweise verzichtet werden kann, wenn er nur unter unverhältnismäßigem Aufwand möglich wäre. In diesem Fall müsste der Aushang der Geschäftsbedingungen am Ort des Vertragsschlusses erfolgen. Diese Ausnahme kommt beim Betreiben des Geoportals nicht zum Tragen. Der Hinweis auf die AGB muss ausdrücklich erfolgen. Er kann unproblematisch elektronisch durchgeführt werden. Darüber hinaus ist die Möglichkeit zur Kenntnisnahme zu verschaffen; dieser Voraussetzung kann etwa durch Bereitstellung einer Downloadmöglichkeit oder durch Zusendung der AGB mittels E-Mail Rechnung getragen werden. Die Einverständniserklärung der Vertragspartei kann ausdrücklich – oder bei fehlendem Formerfordernis konkludent – erfolgen.[58]

Ein praktikabler und auch aus juristischer Perspektive durchführbarer Gestaltungsvorschlag im Hinblick auf die wirksame Einbeziehung von AGB ist exemplarisch anhand folgender Schritte dargestellt:

1. Der Nutzer registriert sich beim Geoportal unter Zuhilfenahme der Identifizierungsfunktion des Elektronischen Personalausweises.
2. Vor der Prüfung sämtlicher Eingaben des Nutzers durch das Geoportal werden diese überblicksartig auf einer Webseite abgebildet. Der Nutzer hat die Möglichkeit, Korrekturen vorzunehmen. Sind sämtliche Daten richtig und vollständig dargestellt, muss eine Schaltfläche betätigt werden, um im Vorgang weiter fortzufahren.
3. Nach Anklicken der Schaltfläche erscheinen die AGB auf der darauf folgenden Webseite. Idealerweise ist eine Schaltfläche „Drucken“ mit entsprechender Funktion implementiert. Am unteren Ende dieser Webseite ist eine Schaltfläche „Nutzungsbedingungen verbindlich anerkennen“ verankert, dessen Betätigung für den weiteren Prozessfortschritt notwendig ist. Es gilt anzumerken, dass das Einverständnis des Kunden in der Regel weder schriftlich noch ausdrücklich erklärt werden muss; vielmehr ist es ausreichend, wenn aus dem Verhalten des Kunden den Umständen nach ein Einverständnis gesehen werden kann. Insofern wäre der Verzicht auf die Schaltfläche „Nutzungsbedingungen verbindlich anerkennen“ aus juristischer Sicht unproblematisch realisierbar.[59] Jedoch führt der ausdrückliche Hinweis auf die Anerkennung der AGB dem im Normalfall juristisch unerfahrenen Nutzer die Tragweite seines Handelns vor Augen. Der Nutzer wird den Inhalt der AGB somit eher zur Kenntnis nehmen, als wenn der Button lediglich mit der Aufschrift „Weiter im Vorgang“ versehen wäre. Es muss im Interesse des Zweckverbands liegen, dass Nutzer nicht gegen AGB verstoßen. Um sich an Bedingungen halten zu können, muss man sie kennen.

Zwar ist es nicht vorgeschrieben, aber als kundenfreundlichen Dienst zu betrachten, dass die AGB zur Nutzung von digitalen Bestandsplänen jederzeit auf der Webseite des Geoportalbetreibers abgerufen werden können. Im Übrigen verringert ein solches Vorgehen die Zahl diesbezüglicher Anfragen durch Kunden.

[58] BeckOK BGB/*Becker*, Ed. 18, Stand 1.2.2007, § 305 Rn. 12 ff.
[59] MüKo BGB/*Basedow*, 5. Aufl. 2007, § 305 Rn. 83.

4.2.4 Abmeldung vom System

Gem. § 13 Abs. 4 Nr. 1 TMG hat das Geoportal zu gewährleisten, dass die Nutzer den Dienst jederzeit beenden können. Um diese Voraussetzung zu erfüllen, kann beispielsweise eine „Logout-Schaltfläche“ implementiert werden. Darüber hinaus muss gem. Nr. 2 eine Löschung sämtlicher personenbezogenen Daten über den Ablauf des Zugriffs grundsätzlich nach Beendigung des Nutzungsvorgangs erfolgen. Es dürfen nur die Daten weiter gespeichert werden, die als Abrechnungsdaten für die Abrechnung des Portaldienstes benötigt werden. Anders ist dies auch, wenn der Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen; in diesem Fall sind die Daten zu sperren. Unter „Sperren“ ist gem. § 3 Abs. 4 Nr. 4 BDSG die Kennzeichnung der personenbezogenen Daten zu verstehen, um deren weitere Verarbeitung oder Nutzung einzuschränken.

5 Sicherheits- und haftungsrelevante Aspekte

5.1 Sicherheitsanforderungen an den Kommunikationsprozess

Dokumente in elektronischer Form sind im Rahmen des E-Government oftmals die einzigen Beweismittel, die dem Empfänger der Erklärung zur Verfügung stehen.[60] Der Austausch von Daten über das Internet mittels Web- oder E-Mail-Dienst ist mit Risiken verbunden: Angreifer können in den ungeschützten Kommunikationsvorgang eingreifen und Daten etwa ausspionieren, abfangen und verändern. Sicherer Informationsaustausch erfordert allgemein Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit und Verfügbarkeit der Daten. Um sämtlichen dieser Anforderungen gerecht zu werden, sind generell verhältnismäßig aufwändige technische und organisatorische Maßnahmen, wie die Verwendung von Signaturverfahren in der Kommunikation, notwendig.

Um die Komplexität der Kommunikationsinfrastruktur auf dem notwendigen Minimum halten zu können, soll der Übertragungsweg nicht durch die elektronische Signaturverfahren abgesichert werden. In Abhängigkeit von der verwendeten Technik wäre u. U. bei sämtlichen Nutzern des Geoportals entsprechende Hardware notwendig, was eine Hürde im Hinblick auf die Inanspruchnahme des Dienstes darstellte. Für das Geoportal selbst besteht in Bezug auf die zu übertragenden Auskünfte dann kein Risiko, wenn in den AGB mittels Ausschlussklauseln verankert ist, dass für Schäden jegliche Haftung ausgeschlossen wird, die etwa durch Manipulationen Dritter an der Kommunikationsverbindung entstehen. Dasselbe muss für Lesbarkeit und Vollständigkeit der Auskünfte gelten.

Zwei der genannten Anforderungen an das Geoportal sind – trotz vorhandener Ausschlussklauseln – von großer Bedeutung. Sie werden nachfolgend kurz aufgezeigt.

5.1.1 Vertraulichkeit

Vertraulichkeit im Rahmen der Kommunikation liegt vor, wenn die ausgetauschten Daten nur berechtigten Personen zugänglich sind.[61] Bei der herkömmlichen ungeschützten Internetkommunikation werden jedoch die ausgetauschten Daten in der Regel über verschiedene Knotenpunkte transportiert, wo sie für geschulte Personen einsehbar sind; dasselbe gilt in Bezug auf den E-Mail-Austausch.[62] Daher fordern sowohl § 13 Abs. 4 Nr. 3 TMG und § 21 Abs. 2 Nr. 1 DSG M-V einen Schutz der Vertraulichkeit der Daten.

Was die Vertraulichkeit des Kommunikationsprozesses anbelangt, vermag durch geeignete Verschlüsselungsverfahren (etwa SSL) die Wahrscheinlichkeit von Manipulationen und des Abfangens der ausgetauschten Daten reduziert zu werden.[63] Eine Verschlüsselung während der Übertragung der Daten ist vorgesehen.

[60] *Roßnagel/Fischer-Dieskau*, NJW 2006, 806 ff.
[61] *Peters/Pinsdorf/Roth*, in: Gitter et al. (Hrsg.), Sicherheit und Rechtsverbindlichkeit mobiler Agenten, 2007, 22.
[62] *Bundesamt für Sicherheit in der Informationstechnik*, Sichere Kommunikation im E-Government, 12 (abrufbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/476846/publicationFile/28061/4_SiKomm_pdf.pdf).
[63] Zur Sicherheit in Kommunikationsnetzen und zur Kryptografie ausführlich *Pfitzmann*, Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme (abrufbar unter: http://dud.inf.tu-dresden.de/~pfitza/DSuKrypt.pdf).

In jedem Fall sind Restriktionen beim Datenzugriff vorzusehen: Personen, die Zugang zu entsprechenden Daten haben, müssen einen vertraulichen Umgang mit ihnen pflegen.[64]

5.1.2 Verfügbarkeit

Die Verfügbarkeit des Systems versteht sich als Nutzbarkeitsgrad der technischen Komponenten. Darunter ist konkret und problembezogen die Erreichbarkeit des Web-Dienstes durch die Nutzer zu subsumieren. Sie wird beeinflusst durch unbeabsichtigte Ausfälle aufgrund technischer Störungen sowie von vorsätzlichen Attacken auf das System durch Außenstehende.[65] Es darf jedoch keine isolierte Betrachtung des Kriteriums Verfügbarkeit stattfinden; sie ist stets im Zusammenhang mit der jeweiligen Anwendung zu vollziehen. Im Falle des Geoportals des ZVG ist der Aspekt der Verfügbarkeit weniger kritisch als etwa bei einem Aktienportal.[66] Dennoch muss aufgrund der vorgesehenen Möglichkeit für Nutzer, den Leitungsbestand tagesaktuell abrufen zu können, eine hohe Erreichbarkeit des Geoportal sichergestellt werden.

5.2 Zugesicherte Gültigkeitsdauer der Auskünfte

Die Richtigkeit der Auskünfte des Geoportals sollte nur für den Tag der Auskunftserteilung zugesichert werden. Im pdf-Format übertragene Auskünfte geben lediglich den Leitungsbestand am Tag der Auskunftserteilung wieder und besitzen Gültigkeit nur für diesen Tag.

Neben der statischen Auskunft, die gewissermaßen ein zum Zeitpunkt der Anfrage aktueller „Snapshot“ des Gebiets, für welches Interesse besteht, darstellt, soll ein dynamischer Webservice bereitgestellt werden, der den Leitungsbestand tagesaktuell abbildet. Der Webservice ist mittels Zugangsdaten des Nutzers stets erreichbar; eingeschränkt ist dieses zusätzliche Informationsangebot jedoch auf zwölf Monate nach Beantragung der Auskunft. Für den Nutzer hat dies zur Folge, dass er das Risiko der Beschädigung oder Zerstörung von Leitungen und Rohren alleine trägt, welche durch Grabungen entstehen, die nach dem Geltungstag der Auskunft vorgenommen werden. Durch die Möglichkeit, mittels des Webservices jederzeit auf aktuelle Leitungsinformationen zugreifen zu können, besitzt der Nutzer ein komfortables Instrument, sich über die Aktualität seiner in pdf-Form vorliegenden Auskunft zu vergewissern. Ist ein geänderter Leitungsbestand zu erkennen, muss vor Beginn der Grabungsarbeiten ein neuer, aktueller Schachtschein eingeholt werden.

In den AGB des Geoportals sind dementsprechende Klauseln mit aufzunehmen. Aus diesen Vertragsbedingungen muss einerseits deutlich hervorgehen, dass sich die erteilte Auskunft unter zugesicherter Korrektheit der Daten nur auf den Ausstellungstag bezieht und sich diese Garantie andererseits ausschließlich auf das pdf-Dokument erstreckt.

Zudem sind in Bezug auf die verschiedenen Leitungsbestände der einzelnen Datenlieferanten – etwa in den AGB – Aussagen über die „Qualität“ der Daten mit aufzunehmen, was zusätzliche Verkehrssicherungspflichten des Bauausführenden auslösen kann; dabei sind unterschied-

[64] *Peters/Pinsdorf/Roth*, in: Gitter et al. (Hrsg.), Sicherheit und Rechtsverbindlichkeit mobiler Agenten, 2007, 22.
[65] *Bundesamt für Sicherheit in der Informationstechnik*, Sichere Kommunikation im E-Government, 11 (abrufbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/476846/publicationFile/28061/4_SiKomm_pdf.pdf).
[66] *Peters/Pinsdorf/Roth*, in: Gitter et al. (Hrsg.), Sicherheit und Rechtsverbindlichkeit mobiler Agenten, 2007, 25.

liche Abstufungen vorzusehen, wie „lageunsicher“ oder „lagesicher“. Liegt eine unsichere Leitungsangabe vor, ist etwa eine Handschachtung zwingend vorzuschreiben.

5.3 Elektronische Aufbewahrung zur Beweissicherung

Die vom Geoportal an Nutzer bereitgestellten Bestandsauskünfte sollen aus Gründen der Beweissicherheit aufbewahrt werden. Beweissicherheit versteht sich als Prognose der größtmöglichen Wahrscheinlichkeit, im Gerichtsprozess eine bestimmte Tatsache zur Überzeugung des Gerichts darlegen zu können.

Aus dem Beweisrecht lassen sich keine Pflichten entnehmen, bestimmte Dokumente und Informationen aufzubewahren. Es muss vielmehr im eigenen Interesse des Zweckverbands liegen, die Beweissicherheit durch Aufbewahrung potenziell relevanter Dokumente und Informationen zu erhöhen, um das Prozessrisiko zu senken. Selbst bei einer fehlenden gesetzlichen Pflicht zur Aufbahrung von elektronischen Dokumenten besteht in vielen Fällen das Bedürfnis, eine beweissichere „Konservierung“ vorzunehmen, um zukünftig in der Lage sein zu können, seine eigenen Rechte durchzusetzen oder bestimmte Tatsachen nachzuweisen.[67]

Ähnlich wie bei beim Kommunikationsprozess sind auch in Bezug auf die rechtssichere Aufbewahrung der erteilten Auskünfte bestimmte grundlegende Anforderungen zu stellen: In diesem Zusammenhang gelten Lesbarkeit, Integrität und Authentizität sowie Vollständigkeit und Verkehrsfähigkeit der geschützten Daten als unabdingbare Voraussetzungen.[68]

Die langfristige Lesbarkeit wird durch die Verwendung standardisierter und gängiger Datenformate sichergestellt. Für Dateien im pdf/a-Format besteht durch die ISO-Zertifizierung die Gewissheit, dass sie auch in Zukunft geöffnet werden können.[69]

Integrität und Authentizität können durch Signaturen und Zertifikate überprüft werden. Der Sicherheitsmechanismus der elektronischen Signatur greift unmittelbar am Dokument: Daten über den Hashwert der Datei stellen den wesentlichen Bestandteil der Signatur dar. Zwar lassen sich Veränderungen an dem Dokument nicht verhindern, jedoch kann – sofern geeignete Signaturverfahren zur Anwendung gelangen – zweifelsfrei bewiesen werden, dass keine Manipulation an den Daten stattfand – wenn dies tatsächlich zutrifft. Beweisrechtlich bieten qualifizierte Signaturen dadurch Vorteile, dass sich der Beweisführer auf den Anscheinsbeweis des § 371a Abs. 1 ZPO berufen kann. Dies ist bei fortgeschrittenen Signaturen nicht der Fall, weil sich für sie keine generellen Angaben zu deren Eignung zur Integritäts- und Authentizitätssicherstellung machen lassen, da beides vollkommen von der Qualität des eingesetzten Verfahrens abhängt.[70] Dennoch können auch mit fortgeschrittenen Signaturen – allerdings aufwändiger – Integrität und Authentizität eines Dokuments nachgewiesen werden: Die Integrität kann über die mathematischen Algorithmen des eingesetzten Hash- und Signaturverfahrens und die Authentizität über die verwendeten Zertifikate belegt werden.

Weitergehend ist auf die Vollständigkeit der Informationen zu achten. Liegen mehrere Dokumente vor, zwischen denen ein innerer Zusammenhang besteht, muss die Dokumentation

[67] *Roßnagel* et al., Langfristige Aufbewahrung elektronischer Dokumente, 2007, 37 ff.
[68] *Roßnagel* et al., Langfristige Aufbewahrung elektronischer Dokumente, 2007, 43 ff.
[69] S. http://www.pdfa.org/doku.php?id=pdfa&DokuWiki=9e479dc870fd3875c70a3179c8ecedff; ausführlich zum pdf/a-Standard *Drümmer/Oettler/von Seggern*, PDF/A kompakt – Digitale Langzeitarchivierung mit PDF, 2007.
[70] *Roßnagel* et al., Langfristige Aufbewahrung elektronischer Dokumente, 2007, 165.

des Gesamtzusammenhangs erhalten bleiben.[71] Sie kann auf überprüfbare Weise sichergestellt werden, indem die zusammengehörige Gesamtheit der Daten mit einer gemeinsamen Signatur versehen werden.

Verkehrsfähigkeit bezeichnet die Möglichkeit, die Daten von einem System auf ein anderes zu übertragen, ohne dass Beeinträchtigungen in der Qualität, Integrität und Authentizität auftreten. Dies wird dadurch erreicht, dass die Schutzmechanismen auf die zu schützenden Daten bezogen sind und nicht nur das schützende System (Zugangs- und Zugriffsschutz) betreffen.

Im Geschäftsverkehr ist in vielen Fällen der Zeitpunkt von Bedeutung, zu dem Geschäftsvorfälle angefallen sind oder abgeschlossen wurden. Nichts anderes gilt für die Archivierung von Dokumenten; sie müssen mit einem Zeitstempel versehen werden, damit im Nachhinein erkennbar ist, welchen Stand das Dokument wiedergibt. Durch den Zeitstempel lässt sich nachweisen, mit welchem Inhalt das Dokument zu einem bestimmten Zeitpunkt vorgelegen hat.

Die vom Geoportal erzeugten Auskunftsdokumente im pdf-Format erhalten direkt nach ihrer Erstellung zum Zwecke der Archivierung – und damit zur Beweissicherung – automatisiert eine qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG. Hierzu gelangt eine sichere Signaturerstellungseinheit gem. § 2 Nr. 10 SigG zum Einsatz. Für derartig signierte Auskunftsdokumente gilt die Beweiserleichterung gem. § 371a Abs. 1 ZPO: Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich durch eine Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist. Auf Auskunftsdokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Regelungen über die Beweiskraft privater Urkunden entsprechende Anwendung. Zwar ist der ZVG, der das Geoportal betreibt, eine öffentlich-rechtliche Körperschaft, dennoch stellen die Auskünfte keine öffentlichen elektronischen Dokumente im Sinne des § 371a Abs. 2 ZPO dar, da das rechtliche Verhältnis zwischen Geoportal und Nutzer kein hoheitliches ist. Außerdem erhält das Dokument einen Zeitstempel, der mittels eines vertrauenswürdigen Dritten generiert wird; es handelt sich dabei um einen Zeitserver der TU Graz. Die Anbringung des Zeitstempels ist somit nicht vom Betreiber des Geoportals beeinflussbar. In der abschließenden Phase im Gesamtprozess der Archivierung wird das Dokument im Dokumentenmanagementsystem (DMS) des ZVG abgelegt.

Durch Signierung der Auskünfte anhand der qualifizierten elektronischen Signatur ist sichergestellt, dass die Integrität und Authentizität der Dokumente bewiesen werden können. Mit dem sofortigen Anbringen des Zeitstempels ist die zu einem bestimmten Zeitpunkt vollzogene Generierung des Auskunftsdokuments belegbar. Beide Faktoren sind für das Gelingen des Nachweises, dass zum Zeitpunkt der Auskunftserteilung ein bestimmter Leitungsbestand vorgelegen hat, unabdingbare Voraussetzungen. Das Ablegen des Auskunftsdokuments in der Archivdatenbank des Dokumentenmanagementsystems hat zur Folge, dass dieses dort unveränderbar gespeichert bleibt.

Sollen die Dokumente längerfristig aufbewahrt werden, ist zur Erhaltung des Beweiswerts eine automatische Übersignierung der signierten Dokumente entsprechend § 17 SigV erforderlich, sobald die verwendeten Algorithmen und Parameter nicht mehr sicherheitsgeeignet erscheinen. Dies lässt sich durch Übersignieren der Hashwerte der archivierten Dokumente

[71] *Roßnagel* et al., Langfristige Aufbewahrung elektronischer Dokumente, 2007, 159.

mit vertretbarem Aufwand realisieren.[72] Dies hat im DMS zu erfolgen und liegt außerhalb der Betrachtung des Geoportals.

[72] S. zum Konzept von ArchiSig *Roßnagel* et al., Langfristige Aufbewahrung elektronischer Dokumente, 2007 sowie RFC 4998 „Long-Time Archiving and Notary Service/Evidence Record Syntax (LTANS/ERS)".