§ 15 Datenschutz bei Geodaten

Meinrad Huser

Literaturauswahl

BALLENEGGER SARAH, KOMMENTIERUNG VON ART. 16 UND 17, IN: MAURER-LAMBROU URS/BLECHTA GABOR P. (HRSG.) BASLER KOMMENTAR, DATENSCHUTZGESETZ, 3. AUFL., BASEL 2014; BELSER EVA MARIA, § 1, 5 und 6, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011; BELSER EVA MARIA/NOUREDDINE HUSSEIN, § 7 und 8, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011;; Bhend Julia/Schneider Jürg, Kommentierung von Art. 10 bis 15, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.) Basler Kommentar, Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 ; Blechta Gabor P., Kommentierung von Art. 3 und 11, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.) Basler Kommentar, Datenschutzgesetz, 3. Aufl., Basel 2014 ; BONDALLAZ STÉPHANE, Le «droit à une télécommunication protégée» ou la nécessité de reconsidérer la protection de la vie privée dans les environnements numériques, Jusletter 25. Februar 2008; BREITENMOSER STEPHAN, Kommentierung von Art. 13 Abs. 1 BV, in: Ehrenzeller Bernhard/Mastronardi Philippe/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die Schweizerische Bundesverfassung, Kommentar, 2. Aufl., Zürich/St. Gallen/Basel/Genf 2008; BRUNNER STEPHAN C./FLÜCKIGER ALEXANDRE, Nochmals: Der Zugang zu amtlichen Dokumenten, die Personendaten enthalten, Jusletter 4. Oktober 2010; BRUNNER STEPHAN C./MADER LUZIUS, Einleitung, in: Brunner Stephan C./Mader Luzius (Hrsg.), Stämpflis Handkommentar zum BGÖ, Bern 2006;; Hürlimann Daniel, Das Google-Urteil des EuGH und die Entfernungspflicht von Suchmaschinen nach schweizerischem Recht, in: www.sui-generis.ch/1; HUSER MEINRAD, Schweizerisches Vermessungsrecht, unter besonderer Berücksichtigung des Geoinformationsrechts und des Grundbuchrechts, 3. Aufl., Zürich/Basel/Genf 2014 (*zitiert*: HUSER, Vermessungsrecht); DERS., Grundzüge des Geoinformationsgesetzes (GeoIG), AJP 2/2010, 143 ff. (*zitiert*: HUSER, Grundzüge); DERS., Geo-Informationsrecht, rechtlicher Rahmen für Geographische Informationssysteme, Zürich 2005 (*zitiert*: HUSER, Geo-Informationsrecht); JÖHRI YVONNE, Kommentierung von Art. 16–25bis und 33 DSG, in: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008; KETTIGER DANIEL, Rechtliche Rahmenbedingungen für Location Sharing Systeme in der Schweiz, Jusletter 9. August 2010 (*zitiert*: KETTIGER, Location Sharing Systeme); DERS., Das schweizerische Geoinformationsrecht im Lichte der Aarhus-Konvention, URP 7/2009, 789 ff. (*zitiert*: KETTIGER, Aarhus-Konvention); DERS., Geheimhaltung und Öffentlichkeit von Geoinformation, Zugangsberechtigung zu Geoinformation im Spannungsfeld entgegenstehender Sicherheitsaspekte, Sicherheit und Recht 1/2009, 53 ff. (*zitiert*: KETTIGER, Geheimhaltung und Öffentlichkeit); DERS., Das neue Geoinformationsrecht im Lichte des Umweltrechts und im Dienste der Nachhaltigen Entwicklung, Umweltrecht in der Praxis 8/2008, 759 ff. (*zitiert*: Kettiger, URP); KLEY ANDREAS/TOPHINKE ESTHER, Kommentierung von Art. 16 BV, in: Ehrenzeller Bernhard/Mastronardi Philippe/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die Schweizerische Bundesverfassung, Kommentar, 2. Aufl., Zürich/St. Gallen/Basel/Genf 2008; MAURER-LAMBROU URS/SCHÖNBÄCHLER MATTHIAS RAPHAEL, Kommentierung von Art. 5, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.) Basler Kommentar, Datenschutzgesetz, 3. Aufl., Basel 2014 ;; Nadakavukaren Schefer Krista, Ein völkerrechtlicher Schutz der kollektiven Privatsphäre? Der Schutz der Privatsphäre und die Anonymität im Zeitalter kommerzieller Drohnen, in: ZSR 2014 Bd I, S. 259 ff.; PROBST THOMAS, Die unbestimmte „Bestimmbarkeit" der von Daten betroffene Person im Datenschutzrecht, Personendaten und anonymisierte Einzeldaten in der globalisierten Informationsgesellschaft – quo vaditis?, AJP 10/2013, 1423 ff. (*zitiert*: PROBST, Bestimmbarkeit); DERS., Die Verknüpfung von Personendaten und deren rechtliche Tragweite, in: EPINEY ASTRID/PROBST THOMAS/GAMMENTHALER NINA, Datenverknüpfung Problematik und rechtlicher Rahmen, Forum Europarecht 18, Zürich/Basel/Genf 2010, 1 ff. (*zitiert*: PROBST, Verknüpfung); RAMPINI CORRADO, Kommentierung von Art. 13, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.) Basler Kommentar, Datenschutzgesetz, 3. Aufl., Basel 2014 ;; ROSENTHAL DAVID, Entwicklungen im privaten Datenschutzrecht (April 2011 bis März 2013), Aktuelle Anwaltspraxis 2013, 707 ff. (*zitiert:* ROSENTHAL, Entwicklungen); DERS., Kommentierung von Art. 3 lit. a und i, 12, 13, 15 und 29 DSG, in: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008; ROSENTHAL DAVID/JÖHRI YVONNE, Kommentierung von Art. 2 DSG, in: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008; RUDIN BEAT, Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, SJZ 105 (2009), 1 ff.; SCHWEIZER RAINER, Kommentierung von Art. 13 Abs. 2 BV, in: Ehrenzeller Bernhard/Mastronardi Philippe/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die Schweizerische Bundesverfassung, Kommentar, 2. Aufl., Zürich/St. Gallen/Basel/Genf 2008; STUDER PETER, Das Öffentlichkeitsgesetz (BGÖ) ist heute ein Werkzeug für investigative Journalisten, Jusletter 11. Dezember 2013; WALDMANN BERNHARD/BICKEL JÜRG, § 12, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011; WALDMANN BERNHARD/HÄNNI PETER, Raumplanungsgesetz, Handkommentar RPG, Bern 2006; WALDMANN BERNHARD/OESCHGER MAGNUS, § 13, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011; WEBER ROLF H., E-Commerce und Recht, rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Aufl., Zürich/Basel/Genf 2010 (*zitiert*: WEBER, E-Commerce und Recht); DERS., Big Data: Sprengkörper des Datenschutzrechts?, Jusletter 11. Dezember 2013 (*zitiert*: WEBER, Big Data); WEBER ROLF H./HEINRICH ULRIKE I., Existiert ein Recht auf Anonymität im Internet?, ZSR 132 (2013) I 477 ff.; WIESTNER Heidi, Informationsbeschaffung durch die Behörden, Umweltrecht in der Praxis 1/2004, 29 ff.

I. Einleitung

Geoinformationen sind Informationen über Objekte und die natürliche oder von Menschen geschaffenen Umwelt die einen Raumbezug aufweisen, wie beispielsweise Landschaftsbilder, **15.1**

Gebäudeanordnungen, Standortkoordinaten, Ortsnamen oder Postadressen. Soweit sie in digitaler Form aufgezeichnet sind, werden sie „Geodaten“ genannt. Geografische Informationen spielen *im Alltag eine grosse Rolle*. Menschliche Aktivitäten finden an einem bestimmten Ort statt. Menschen sind Mitglied einer Gemeinschaft (wie etwa Nationalität, Familie oder Sportclub), die mit konkreten Landflächen oder Wohn- oder Spielorten identifiziert werden. Wer von einer Person spricht, stellt diese – ausdrücklich oder stillschweigend – in einen geografischen Kontext. Personen sind somit immer mit geografischen Informationen verknüpft. Umgekehrt kann jedoch eine geografische Information durchaus für sich stehen, ohne einer bestimmten Person zugeordnet zu sein. Ein Wegweiser etwa zeigt dem Wanderer die Höhenlage sowie die Richtung und den Zeitaufwand bis zum Berggipfel. Eine Sachinformation etwa über ein Gebäude kann aber Teil von Personeninformationen werden, wenn sie mit einer Adressliste der Gebäudeversicherungsanstalt verknüpft wird.

15.2 Sowohl im privaten als auch im öffentlich-rechtlichen Bereich stellen systematisch gesammelte und digitalisierte *Geoinformationen* mit Personenbezug eine *wichtige Informationsquelle* dar. Zu denken ist etwa an Register mit Unternehmeradressen, an das Grundbuch mit Eigentümerangaben, aber auch an digitalen Landeskarten mit Ausflugsrestaurants. In allen Bereichen hat die technologische Entwicklung die Suche nach Informationen über konkrete Personen beschleunigt und den Einsatz von Verzeichnissen und Datensammlungen vereinfacht. Die Technologie erleichtert zudem die Möglichkeiten, Datenbankinhalte zu verknüpfen und daraus ohne grossen Aufwand neue Informationszusammenstellungen zu schaffen.

15.3 Im privaten bzw. kommerziellen Bereich vereinfachen und beschleunigen mobile Geräte, wie Smartphones oder Tablet Computer, den *Informationszugang*. Solche Endgeräte dienen als Navigationssysteme leiten zu Sehenswürdigkeiten in der näheren Umgebung. Gleichzeitig liefert aber das benutzte System dem Anbieter auch zwingend (evtl. automatisch) seinen Standort und ermöglicht diesem, unbestellte, ortsbezogene Werbung zuzustellen. Geräte und Sammlungen mit digitalen Geodaten sind auch für private Nutzer (Sportveranstalter, weltweit tätige Firmen) unabdingbare Hilfsmittel bei der Planung und Organisation.

15.4 Bei den Behörden und der öffentlichen Verwaltung ermöglicht die moderne Technologie eine effizientere und gleichzeitig differenziertere Bewirtschaftung des Bodens. Moderne Geoinformationssysteme (GIS) erlauben den zuständigen Amtsstellen, die für ihre Tätigkeit benötigten Rauminformationen schnell und anwenderfreundlich abzurufen und zur Verfügung

zu stellen. Dementsprechend finden solche Geoinformationssysteme bei vielen Staatsaufgaben mit Raumbezug Anwendung, v.a. aber in der Stadt- und Raumplanung, bei der Landestopographie sowie beim Umwelt- und Ressourcen-Management.

Die *Rechtsfragen* bei der Verwendung der Geoinformationen in digitaler Form *sind komplex*. **15.5**
Bei der Lösungssuche ist zunächst die Datenschutzrelevanz der Sachinformationen zu bestimmen (unten Rz 15.6 ff.). Für Geoinformationen, die den Persönlichkeitsschutz verletzen könnten, sind dann die konkreten Anforderungen zu besprechen. Aufgrund der Rechtslage drängt sich eine Unterscheidung zwischen Geodaten (unten Rz 15.60 ff.) und Geobasisdaten (unten Rz 15.97 ff.) auf. Wie sich der Einzelne gegen ungerechtfertigte Verwendung seiner persönlichen Geodaten wehren kann, wird am Schluss für beide Rechtsbereiche gemeinsam besprochen (unten Rz 15.133 ff.).

II. Die Datenschutzrelevanz von Geodaten

1. Geodaten und Datenschutzgesetz

Datenschutz bedeutet Schutz der Persönlichkeit und der Grundrechte von Personen, über die **15.6**
Daten bearbeitet werden (Art. 1 DSG). Geodaten sind geografische Informationen in digitaler Form, die mit einem bestimmten Zeitbezug die Ausdehnung und Eigenschaften bestimmter Räume und Objekte beschreiben (Art. 3 Abs. 1 lit. a GeoIG). Diese raumbezogenen Daten sind Sachdaten. Es stellt sich zunächst die Frage, warum das Bearbeiten solcher *Sachdaten* überhaupt *Gegenstand des Datenschutzes* sein kann.

a) Angaben über bestimmte oder bestimmbare Personen

aa) Im Allgemeinen (Art. 2 und 3 lit. a DSG)

Das Datenschutzgesetz erfasst unter dem Begriff *Personendaten* alle Angaben, die sich auf **15.7**
eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG).

Eine Person ist bestimmt, wenn sich die Identifikation aus der Information selber ergibt[1], **15.8**
wenn sich die Angaben einer oder mehreren Personen zuordnen lassen. Dies ist bei den Informationen zur Person des Grundeigentümers oder eines dinglich Berechtigten/Verpflichteten (Wegrechtsberechtigte Person)[2] offensichtlich der Fall, bei beschreibenden Geodaten jedoch eher nicht.

15.9

1 BGE 138 II 346 E. 6.1; 136 II 508 E. 3.2 S. 514; ROSENTHAL, Art. 3 lit. a DSG N 24 ff.; BELSER/NOUREDDINE, § 8 N 39 ff.; PROBST, Bestimmbarkeit, 1425 und 1429 ff.

2 Gestützt auf Art. 970 Abs. 2 und 3 ZGB, Art. 26 Abs. 1 GBV sowie GeoIV Anhang, Identifikator 7.

Eine Person ist bestimmbar, wenn sie nicht aus der Geoinformation selber, sondern nur aus dem Kontext und im Verbund mit zusätzlichen Informationen erkannt werden kann[3]. Entscheidend sind dabei nicht die theoretische Möglichkeit der Identifizierung, sondern der konkrete Aufwand und auch das Interesse, das jemand an der Identifizierung einer gewissen Person hat.

bb) Zum Aufwand der Rückschlüsse auf konkrete Personen

15.10 Lässt sich aus Sachdaten *mit geringem Aufwand Rückschlüsse auf konkrete Personen* ziehen, besteht ein Indiz für die Anwendbarkeit des Datenschutzgesetzes. Der Aufwand ist unverhältnismässig, wenn "nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen Aufwand auf sich nehmen wird (etwa durch komplizierte Analyse einer Statistik)"[4].

15.11 Ob der Aufwand unverhältnismässig ist, hängt in jedem Fall auch von den *Möglichkeiten und den technischen Kenntnissen der Person*, welche die Daten bearbeitet[5]. Hoch entwickelte Techniken vereinfachen die Verknüpfung von Datenbanken[6] und ermöglichen mit wenig Aufwand oder gar automatisch Rückschlüsse auf bestimmte Personen. Die Technik übernimmt – gestützt durch das Internet – die Suche nach Personen und anderen Sachdaten, die einen Personenbezug zulassen (Stichwort Big Data[7]). Das Kriterium des Aufwands allein hilft kaum, die Datenschutzrelevanz von Sach- oder Geodaten definitiv zu bestimmen.

cc) Zum Identifikationsinteresse

15.12 Ob der Aufwand verhältnismässig ist, beurteilt sich auch nach dem *Interesse*, das jemand *an der Identifizierung einer Person* hat[8]. Geodaten und andere Sachdaten können aus dieser Sicht einmal datenschutzrelevant sein und ein anderes Mal gerade nicht[9]. Auch wenn erst der Empfänger die betroffene Person zu identifizieren vermag[10], bleibt der Datenlieferant nach

---

3 Siehe die Zusammenfassung der Voraussetzungen für die Bestimmbarkeit in BGE 138 II 353 f., E. 6.1; s.a. ROSENTHAL, Art. 3 lit. a DSG N 20; s.a. oben Rz 3.30 ff., insbes. Rz 3.38, wo auf die Praxis verwiesen wird, dass eher zugunsten der Personendaten entschieden wird und der Praktiker seine Argumentation sinnvollerweise auf die Anwendung des materiellen Datenschutzrechts konzentrieren soll.

4 BSK DSG-BLECHTA, Art. 3 N 11, ebenso ROSENTHAL, Art. 3 lit. a DSG N 24.

5 BGE 136 II 514; ROSENTHAL, Art. 3 lit. a DSG N 25.

6 PROBST, Verknüpfung, 3 f.

7 Big Data bezeichnet eine grosse Datenaggregation, die es erlaubt, aus reinen Sachdaten Schlüsse auf Personen zu ziehen (so jedenfalls WEBER, Big Data, Rz 8).

8 ROSENTHAL, Art. 3 lit. a DSG N 25; PROBST (Bestimmbarkeit, 1431 ff.) untersucht diese Frage anhand verschiedener „Beurteilungshorizonte".

9 Siehe dazu Fallbeispiel bei PROBST (Bestimmbarkeit, 1430), der die Konsequenzen aus dem Urteil Logistep AG (BGE 136 II 508) darstellt und fragt, ob die Abgrenzung zwischen Personendaten und Nicht-Personendaten in einer globalisierten Informationsgesellschaft tatsächlich allmählich zu verflüchtigen droht (PROBST, Bestimmbarkeit, 1424). Für IP-Adressen s. ROSENTHAL, Art. 3 lit. a DSG N 40.

10 BGE 136 II 515; ROSENTHAL, Art. 3 lit. a DSG N 24 f.

der Rechtsprechung[11] an seine datenschutzrechtlichen Pflichten gebunden. Der Einzelfall ist zu beachten. Das vermag für die Rechtsanwendung zwar Unsicherheiten bringen, ermöglicht jedoch eine Interessenabwägung mit der Folge, dass die Datenschutzgesetzgebung zielgerichtet angewandt wird und das Datenbearbeiten nur (aber immer) dann beschränkt ist, wenn tatsächlich konkrete Personen betroffen sind[12]. Dennoch macht es Sinn, mit PROBST den Gesetzgeber[13] zu fragen, für welche Kategorien von Nutzern die Bestimmbarkeit gegeben sein muss, damit Geodaten datenschutzrelevant werden können[14].

b) Zuordnung von Geodaten zu den Personendaten? [15]

Die Datenschutzrelevanz von Sachdaten hat das Bundesgericht im Urteil vom 31. Mai 2012 **15.13**
für die *Bildaufnahmen von Street-View* präzisiert. Die Bilder, die mit Kameras auf speziell ausgerüsteten Autos aufgenommen wurden, zeigen nicht nur Strassenzüge, sondern auch dort anwesende Personen mit ungenügend oder gar nicht verwischten Gesichtern sowie Nummernschilder geparkter oder vorbeifahrender Fahrzeuge. Die Aufnahmen geben auch den Blick frei in Gärten und Balkone oder in das Innere von Wohnhäusern ohne Personenabbildungen. Aufnahmen wurden als Personendaten qualifiziert, „[…] wenn sich Bilder von Häusern oder Fahrzeugen der Wohnadresse einer bestimmten Person zuordnen lassen und damit Rückschlüsse auf die konkrete Lebenssituation von Bewohnern des Hauses oder des Halters eines Fahrzeugs (sofern das Nummernschild erkennbar ist) möglich sind“[16]. Weil keine Empfehlung des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vorlag, hatte das Bundesgericht die Frage nicht diskutiert, ob auch Häuserfassaden ohne Einblick ins Gebäudeinnere aus datenschutzrechtlichen Gründen verschleiert werden müssten. Die Rechtsprechung muss bei der Beurteilung der Geodaten kritisch gewürdigt werden. Es ist

11 Bundesgericht: „Dies bedeutet für den vorliegenden Fall, dass nicht vorausgesetzt ist, dass die Urheberrechtsverletzer bereits für die Beschwerdegegnerin bestimmbar sind. Vielmehr genügt es, wenn sie es nach Übergabe der entsprechenden Daten für die Urheberrechteinhaber werden. Trifft dies zu […], so gelangt das Datenschutzgesetz indessen auch auf die Beschwerdegegnerin selbst zur Anwendung. Anders entscheiden würde bedeuten, das Datenschutzgesetz nur auf die einzelne Empfänger anzuwenden, nicht aber auf die Person, welche die betreffenden Daten beschafft und sie verbreitet. Dies würde dem Zweck des Gesetzes zuwiderlaufen“ (BGE 136 II 515).

12 Wegweisend § 4 Gesetz vom 24. Mai 2011 über die Geoinformation im Kanton Aargau (Kantonales Geoinformationsgesetz, KGeoIG; SAR 740.100), der das Datenschutzrecht nur dann zur Anwendung bringt, soweit Geodaten einer bestimmten oder bestimmbaren Person zugeordnet werden können.

13 PROBST (Bestimmbarkeit, 1431) leitet die Lösungsvorschläge aus dem Unionsrecht ab, weil das DSG dazu keinen Antworten liefert. Er bezeichnet seine konkreten Vorschläge als ersten Schritt zur Problemlösung (PROBST, Bestimmbarkeit, 1436).

14 PROBST, Bestimmbarkeit, 1436; auch WEBER (Big Data, Rz 9 f., 23) sieht bei der Entwicklung der Technik das Konzept der Erfassung von Personendaten in Frage gestellt. Nach diesem Autor (Big Data, Rz 57) treten neue Elemente in den Vordergrund, etwa die Sicherstellung der Kompatibilität von Datenverarbeitungen mit der ursprünglichen Zweckbestimmung, die Ausrichtung datenschutzrechtlicher Normen auf eine sachgerechte Risikoorientierung (organisatorische und technische Massnahmen), die Schaffung einer angemessenen Data-Governance-Kultur sowie die Implementierung von Rechenschafts- und Verantwortungsprinzipien («Accountability»). Solche Konzepte gehen über die traditionellen Datenschutzgesetze hinaus und verlangen sowohl eine breite, zivilgesellschaftliche Diskussion über die Legitimität von Datenbearbeitungen als auch eine intellektuelle Offenheit für ein neues weit verstandenes Datenrecht.

15 Zu den Sachdaten mit Personenbezug s.a. eingehend unten Rz 28.126 ff.

16 BGE 138 II 355 E. 6.3; s.a. oben Rz 14.9 ff.

dabei zwischen Geodaten als eigenständige Informationen über den Boden und die Umwelt und Geodaten als Teil kombinierter Informationen zu unterscheiden.

Geodaten sind für sich genommen *weder bestimmt noch geeignet, Rückschlüsse auf Personen zu ziehen*, auch wenn sie örtliche Gegebenheiten darstellen oder Ortsangaben machen. Bilder von Gärten, Höfen, Balkonen oder Hausfassaden und Wohnbereiche können die Lebensweise oder den Wohlstand der Bewohner an einem bestimmten Ort vermitteln; nicht die Person, sondern die bebaute und unbebaute Natur ist das Thema der Geodaten. **15.14**

Einer Fotoaufnahme allein ist nicht zu entnehmen, wer dem abgebildeten Reichtum frönt oder in diesem einfachen Bau haust. Solche *Geodaten bleiben Sachdaten*, auch wenn sie in einem Informationssystem oder einer Datenbank gesammelt sind und sich mittels moderner Informatiktechnologie recht einfach bearbeiten lassen. Aus Geodaten allein kann – ohne ergänzende Angaben aus einer anderen Datenquellen – nie auf konkrete Personen geschlossen werden und zwar auch dann nicht, wenn Koordinaten oder Ortsangaben miteinander verknüpft werden[17]. Diese Feststellung können auch oft erwähnte Beispiele nicht in Abrede stellen[18]. **15.15**

Werden *Geodaten mit anderen Informationen kombiniert* bzw. als Datenquelle oder als Georeferenzinformation in Informationssystemen integriert, ist die Datenschutzrelevanz des neuen Produkts eigenständig zu beurteilen. Keine Rückschlüsse auf Personen können Kombinationen liefern, die nur aus Geodaten oder Geobasisdaten zusammengesetzt sind. Der neue Datensatz ist nicht datenschutzrelevant[19]. Geodaten bleiben auch bei Verknüpfungen Sachdaten, mutieren also nicht zu Personendaten[20]. Ergänzen sie Daten, die Rückschlüsse auf konkrete Personen ermöglichen, ergibt sich die allfällige Datenschutzrelevanz nicht aus dem Gehalt der Geodaten, sondern aus den weiteren Datenquellen (Unternehmerregister, Einwohnerregister[21], Telefonbuch oder Adresssammlung usw.), die ihrerseits datenschutzrelevant sein können[22]. Der ursprünglichen Datenquelle kommt in Kombination **15.16**

17 Die in der Literatur erwähnten Beispiele lassen die Identifikation immer nur aufgrund der Hinweise aus personenbezogenen Informationen zu: Beim Einblick ins Gebäudeinnere (BGE 138 II 355 E. 6.3) ist vorausgesetzt, dass der Bewohner aufgrund der Wohnadresse ausfindig gemacht werden kann. Wenn ein anonymes Unternehmen mit Sitz in Vevey mit einem Jahresumsatz von über einer Million erwähnt ist (Beispiel bei PROBST, Verknüpfung, 19), gelingt die Identifikation nicht aufgrund der Ortsangabe, sondern nur wegen der Unternehmensbeschreibung und allenfalls einer Konsultation des Handelsregisters.

18 Beim Einblick ins Gebäudeinnere (BGE 138 II 355 E. 6.3) ist vorausgesetzt, dass der Bewohner aufgrund der örtlichen Lage und mittels Wohnadresse ausfindig gemacht werden kann. Wenn ein anonymes Unternehmen mit Sitz in Vevey mit einem Jahresumsatz von über einer Million erwähnt ist – Beispiel bei PROBST, Verknüpfung, 19 – gelingt die Identifikation nicht aufgrund der Ortsangabe, sondern nur wegen der Unternehmensbeschreibung und allenfalls einer Konsultation des Handelsregisters.

19 Diese Aussage wird nicht geteilt (WEBER, Big Data, Rz 8).

20 So auch PROBST, Verknüpfung, 6.

21 Registerharmonisierungsgesetz mit seinen Verknüpfungen von Sach- und Personeninformationen: das Standesregister (Infostar), das zentrale Migrationsinformationssystem (ZEMIS) des Bundesamtes für Migration, das Informationssystem „Ordipro“ des Eidgenössischen Departements für auswärtige Angelegenheiten, das im Informationssystem VERA (vernetzte Verwaltung der Auslandschweizerinnen und Auslandschweizer) geführte Matrikelregister, das zentrale Versichertenregister, das zentrale Rentenregister und das Sachleistungsregister der Zentralen Ausgleichskasse sowie die kantonalen und kommunalen Einwohnerregister und Stimmregister (Art. 2 RHG).

22 So auch PROBST, Bestimmbarkeit, 1425.

mit verschiedenen Daten keine eigene oder – wegen der eingesetzten Technik[23] - neue Bedeutung zu. Die Einhaltung der datenschutzrechtlichen Vorgaben ist deshalb einzig beim zusammengesetzten Datensatz zu prüfen. Konsequenterweise können Geodaten auch nicht dem Datenschutz unterstellt sein, nur weil sie geeignet sind, Teil einer datenschutzrelevanten Kombination zu sein. Allgemeine Risiko- und Wahrscheinlichkeitsannahmen[24] helfen ebenso wenig weiter, wie die Anregung, dass Geodaten im Zweifelsfall nach den Regeln der Personendaten zu behandeln seien. Entscheidend ist einzig die Möglichkeit aus der konkreten Gesamtinformation Rückschlüsse auf konkrete Personen zu ziehen.

15.17 Soweit Geodaten *öffentlich zugängliche Bereiche* als Gesamtbild – unabhängig ob mit Spezialgeräten oder aus der Luft – einfangen, ist kaum zu verhindern, dass nicht auch Personen oder Identifikationsmerkmale mitenthalten sind. Es werden deshalb wohl die meisten Aufnahmen im öffentlichen Raum datenschutzrelevant sein.

c) Bedeutung der Technik

aa) Im Allgemeinen

15.18 Der Aufwand, um aus Sachdaten auf bestimmte Personen schliessen zu können, wird mit der Entwicklung der Technik immer einfacher[25]. Dies wird wohl dazu führen, dass dem Kriterium des Aufwands für die Frage der Bestimmbarkeit einer konkreten Person keine Bedeutung mehr zukommt. Die *Technik* nimmt somit je länger je mehr eine *eigenständige Funktion* beim Erfassen und Bearbeiten von Geoinformationen ein. Ob ihr aber selber Datenschutzrelevanz zukommt, muss geklärt werden.

15.19 Der Gesetzgeber war sich bereits 1988 der kommenden *Entwicklung der Technik* und der damit verbundenen Herausforderungen für den Persönlichkeitsschutz bewusst. Die Botschaft zum Datenschutzgesetz hielt fest: "Ein allgemeines Datenschutzgesetz kann […] nicht alle denkbaren Ausprägungen der Datenbearbeitung berücksichtigen; es muss vielmehr allgemeine, grundsätzliche Regeln enthalten, die es erlauben, die meisten Probleme wenigstens im Ansatz zu bewältigen, und daneben Raum für die Weiterentwicklung des Datenschutzes lassen"[26]. Das Gesetz soll gegenüber der Technik und ihrer Entwicklung also möglichst neutral bleiben[27]. Ob diese Aussagen heute noch geteilt werden, ist offen. Die Technik erhebt und verknüpft heute – zwar mit den Ideen des Menschen programmiert, aber trotzdem ohne Zutun eines Menschen im Einzelfall – Geodaten mit weiteren Daten und

---

23 Huser, Geo-Informationsrecht, 171 f.
24 Statt vieler PROBST, Verknüpfung, 18 f., 23.
25 S.a. oben Rz 15.2 f.
26 Botschaft DSG 1988, 431 f.
27 Botschaft DSG 1988, 432; s.a. oben Rz 1.26

ermöglicht Rückschlüsse auf konkrete Personen. Kommt diesem „eigenständigen" Datenbearbeiter deshalb – anders als noch 1988 – heute eine neue Rolle beim Schutz der Privatsphäre zu?

bb) Für das Bearbeiten von Daten

15.20 Da der Gesetzgeber den Schutz der Persönlichkeit nicht an der eingesetzten Technik anknüpft, macht das Gesetz *keine Aussagen über die Zulässigkeit solcher Hilfsmittel*. Drohnenflüge (unbemannte ferngesteuerte Luftkörper) sind nicht Gegenstand des Datenschutzgesetzes. Auch die Entwicklung der Aufnahme- oder Wiedergabegeräte ist nicht datenschutzrelevant, und zwar auch dann nicht, wenn Aufnahmen aus immer weiterer Entfernung aussagekräftigere Informationen liefern können (Luftbilder aus Flugzeugen oder von Satelliten). Mit den Instrumenten des Datenschutzgesetzes lässt sich jedenfalls der Einsatz technisch hoch sensibler Geräte auch dann nicht auf Vorrat verhindern, wenn etwa unerlaubtes Aufnehmen oder rechtswidriges Bearbeiten der Daten befürchtet wird. Der Datenschutz hindert nicht den Einsatz einer Drohne, sondern beurteilt das erstellte Produkt, setzt also bei der Frage an, ob mit dem Einsatz Personen identifiziert werden können. Vermessungsaufnahmen beispielsweise dürfen mit äusserst genauen technischen Hilfsmitteln erfolgen; erst wenn sie Rückschlüsse auf konkrete Personen zulassen, ist ihr Ergebnis (nicht ihr Einsatz) nach den Grundsätzen des Datenschutzes zu beurteilen. Zu Recht hat deshalb das Bundesverwaltungsgericht anerkannt, dass Drohnenaufnahmen im Rahmen der zollrechtlichen Überwachung eines 25 km breiten Grenzstreifens[28] erst dann datenschutzrelevant werden, wenn sie Personen (beim illegalen Grenzübertritt) erfassen. Bei Drohneneisätzen zur Überwachung von Sportveranstaltungen[29] wird hingegen der Fokus direkt auf randalierende Menschen gerichtet. Der Einsatz der Drohnen für solche Aufnahmen ist ohne Zweifel unmittelbar datenschutzrelevant und untersteht den Bearbeitungsgrundsätzen der Datenschutzgesetze.

cc) Beim Beschaffen von Beweismitteln

15.21 Die digitale *Technik* bietet in verschiedenen Lebensbereichen neue Einsatzmöglichkeiten, namentlich auch *zur Überwachung* konkreter Orte. Dass dies mit dem Datenschutz kollidieren

28 Dazu BVGer A-2482/2007 vom 26. Juni 2007, E. 3.2, wo das Bundesverwaltungsgericht feststellt, dass das Zollgesetz für den Einsatz von Drohnen zur Überwachung eines Grenzstreifens eine ausreichende gesetzliche Grundlage bietet.

29 Das Bundesamt für Zivilluftfahrt hatte Korridore für den Einsatz von Überwachungsdrohnen anlässlich der Fussballeuropameisterschaften 2008 in der Schweiz, genehmigt, was zu einem Verfahren mit Entscheid des Bundesverwaltungsgerichts vom 12. Juni 2008, betr. provisorische Verfügung (A-3614/2008) geführt hatte.

kann, ist offensichtlich[30]. Entsprechende Fragen haben auch das Bundesgericht bereits mehrmals beschäftigt. Das höchste Gericht kam dabei unter anderem zum Schluss, dass der Einsatz von Kameras zur Überwachung des Arbeitsplatzes dem Arbeitsrecht (Art. 26 Abs. 1 ArGV3) widerspreche. Eine Überwachung der Umgebung des Arbeitsplatzes (Art. 26 Abs. 2 ArGV3)[31] oder der Aussendiensttätigkeit von Taxifahrern[32] mit Kameras oder mit der GPS-Technik könne jedoch durchaus erlaubt sein, wenn dies gesetzlich vorgesehen ist und insbesondere dem Verhältnismässigkeitsprinzip entspreche. Erforderlich sei immer eine Interessenabwägung.

15.22 Doch nicht jede allgemeine gesetzliche Grundlage genügt, um die notwendigen Beweismittel rechtmässig zu erheben; das Gesetz, das zur Überwachung den Einsatz der Technik anordnet, muss nicht nur *formell,* sondern auch *inhaltlich rechtmässig* sein. Es muss namentlich die Grundrechte der Bundesverfassung und die durch die Europäischen Menschenrechtskonvention (EMRK) geschützten Rechte einhalten. Das Bundesgericht hatte in diesem Sinn 2008 eine Bestimmung des zürcherischen Polizeigesetzes als unzulässig beanstandet, die auf Anordnung irgendwelcher Polizisten eine totale Überwachung des öffentlichen und „halböffentlichen" Raumes mit hochpräzisen Kameras und weiteren technischen Gerätschaften ermöglicht hätte. „Das Fehlen von jeglichen Zweckangaben verunmöglicht es von vornherein, klare Ziele und ein öffentliches Interesse an entsprechenden Überwachungsmassnahmen zu ermessen"[33].

dd) Beim Gewähren des Zugangs

15.23 Bei der Gewährung des Zugangs zu Geoinformationen ist die *datenschutzrechtliche Bedeutung* zweier *technischer Erscheinungsformen* zu diskutieren: die Geoportale und die Adressen (E-Mail-Adressen; IP-Adressen).

15.24 *Geoportale* ermöglichen den Zugang zu einer oder zu verschiedenen Datensammlungen. Sie vermitteln den Zugang zur Informationsquelle. Soweit sie keine Inhalte transportieren, erfüllen sie einzig die Funktion als Zugangsvermittler (Access-Provider). Als reine Türöffner unterstehen sie der Datenschutzgesetzgebung an sich nicht. Diese kommt aber zur Anwendung, sobald Metadaten, etwa Angaben über die Informationssuchenden oder deren Adressen und Codenummer registriert – was im online-Verkehr unabdingbar ist –, und bearbeitet werden. Ist mit dem Zugang zu einer Web-Site ein direkter oder (mit einem

---

30 S.a. oben Rz 11.72 ff. und Rz 13.170 ff. sowie unten Rz 17.20 ff. und Rz 17.61 ff.

31 BGE 130 II 425, 434 E. 4.2; S.a. unten Rz 17.66

32 BGer 2C_116/2011 vom 29. August 2011, E. 8; 2C_117/2011 vom 29. August 2011, E. 8; 2C_118/2011 vom 29. August 2011, E. 8.

33 BGE 136 I 87 E. 8.

Mausklick) indirekter Zugriff auf die Inhalte verbunden, vermittelt das Geoportal auch Inhalte. Das Geoportal ist damit Teil der Übertragungskette, und deren Betreiber wird – wie der Content-Provider – direkt verantwortlich für den Datenschutz[34]. In aller Regel sind deshalb die Geoportale datenschutzrelevant, sobald Metadaten gespeichert werden oder der Zugang zu datenschutzrelevanten Inhalten vermittelt wird. Wie weit nur schon das Bereitstellen von Links als Bearbeiten (von Geodaten) bezeichnet werden kann, ist zu klären, nachdem der europäische Gerichtshof[35] einen datenschutzrechtlichen Anspruch auf Unterbinden von Links anerkannt hat[36].

15.25 Die *Mitverantwortung des Zugangsvermittlers* deckt sich im Übrigen mit der strafrechtlichen Verantwortung nach Art. 322bis StGB (Nichtverhindern einer strafbaren Veröffentlichung) und den Pflichten der Internetanbieter nach Art. 14 Abs. 4 BÜPF (zur Identifikation des Urhebers einer Straftat im Internet)[37].

15.26 *E-Mail-Adressen* sind das Postfach im Internet und einer bestimmten Person zugewiesen. Nach der Rechtsprechung sind solche Adressen Personendaten[38]. Für die Frage der Datenschutzrelevanz von Geodaten haben sie aber keine Bedeutung. Sie sind „Briefkästen in der virtuellen Welt" und informieren nicht über Standorte von Personen. Ihnen fehlt auf jeden Fall der Ortsbezug.

15.27 Die *IP-Adresse* (Internet-Protokoll-Adresse[39]) benennen Endgeräte, die an ein Internet-Netzwerk angeschlossen sind. Auf der Grundlage dieser Adresse kann der Standort des Gerätes ermittelt werden. Diese Adressen können Personenangaben enthalten, weil das Gerät einem bestimmten Nutzer zugewiesen ist[40]. Bei einer funktionalen Sichtweise[41] sind diese Angaben datenschutzrelevant. Die IP-Adresse gibt aber nur die Identität und allenfalls den Standort[42] des Rechners bekannt. Sie vermag die natürliche Person, der die Adresse und damit die Verantwortung zugeschrieben werden kann, jedoch nicht mit der nötigen Sicherheit bestimmen[43]. Die IP-Nummer ermöglicht die Personenidentifikation erst, wenn sich der

---

34 Vergleichbar mit dem Sachverhalt in BGE 136 II 515.

35 Gerichtshof der Europäischen Union, Pressemitteilung Nr. 70/14, Luxemburg, 13. Mai 2014, Urteil in der Rechtssache C-131/12, Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González.

36 Die eigentliche Quellinformation, auf welche verlinkt wurde, bleibt aber weiterhin bestehen (dazu MARKUS DORMANN/LUKAS FÄSSLER, Google Urteil – Das „Recht, im Internet vergessen zu werden Müssen Suchmaschinen Links auf persönliche Daten löschen?, veröffentlicht auf ‹www.fsdz.ch› [besucht am: 10. September 2014]).

37 BGE 139 IV 98, 99; s.a. oben RZ 9.84 ff.

38 VPB 96.106 E. 2.4, s. die bedenkenswerten Vorbehalte bei ROSENTHAL, Art. 3 lit. a DSG N 40; s.a. oben Rz 9.84.

39 Grundlegend oben Rz 9.77 ff. mit kritischen Bemerkungen zum Rechtsprechungsergebnis.

40 WEBER unterscheidet zwischen den statischen IP-Adressen, die auf Dauer vergeben werden, und den dynamischen Adressen, die nur temporär die Einwahl ins Internet ermöglichen (E-Commerce und Recht, 470 f.; WEBER/HEINRICH, 484), eine Unterscheidung, die aber für die Datenschutzrelevanz kaum von Bedeutung ist.

41 So BVGer A-3144/2008 vom 27. Mai 2009 E. 2.2.4.

42 Bei der Internettelefonie kann von jedem Ort der Welt telefoniert werden, ohne dass der Standort des Geräts ermittelt werden kann. Dies verunmöglicht jedoch die Rückverfolgung von Notrufen, was zurzeit ein Verstoss gegen das Fernmeldegesetz darstellt und wohl zu einer Anpassung des Gesetzes führen wird, weil niemand die technische Innovation behindern wolle (so wird der Vizedirektor des Bundesamtes für Kommunikation in der NZZ am Sonntag vom 23. März 2014, 63, zitiert).

43 Überzeugend ROSENTHAL, Art. 3 lit. a DSG N 26 f.

Bezug durch Zusatzinformationen (wie Domain Name, aus Angaben der Website selbst oder durch Konsultation der entsprechenden Verzeichnisse[44]) herstellen lässt. In der Regel entsteht ein Bedarf[45] nach Identifikation der verantwortlichen Person[46] erst, wenn eine Straftat verübt wird. Denn in diesem Moment muss die Person, der die Adresse zugeteilt ist, bekannt gegeben werden (Art. 14 Abs. 4 BÜPF). Erst jetzt ist die Person bestimmt und wird vom Datenschutz erfasst. „Dadurch werden die betreffenden Aufzeichnungen des Webservers automatisch zu Personendaten auch bezüglich der so ermittelbaren bzw. ermittelten Person und nicht mehr nur des registrierten Inhabers der IP-Adresse“[47].

ee) Bedeutung der technischen Geräte zum Bearbeiten von Geodaten

15.28 Bei der *Darstellung flächendeckender Geoinformationen* kommen verschiedene technische Hilfsmittel zum Einsatz. Bekannt sind das GPS (deutsch: Globales Positionsbestimmungssystem) und die „Location Sharing Systeme“.

15.29 *GPS-Technologie* wird eingesetzt, um den Standort des Gerätes zu bestimmen und den Weg zum Ziel zu finden. Aufnahmen von GPS-Geräten können als Beweismittel für den Aufenthalt eines Arbeiters[48] oder für den Fluchtweg mit einem Auto dienen. In verschiedenen Verwaltungs- und Gerichtsentscheiden werden die Aussagen dieser Geräte über gefahrene Routen als Beweismittel berücksichtigt[49]. Damit geht das Gericht offensichtlich von der Zulässigkeit der mit den technischen Hilfsmitteln erhobenen Beweismittel aus. Datenschutzrechtliche Bedenken sind aus den Urteilen jedenfalls nicht herauszulesen. Aber auch hier gilt: Nicht der Einsatz des GPS-Gerätes, sondern seine Aufzeichnungen sind datenschutzrelevant.

15.30 *Location Sharing Systeme* sind standortbezogene Dienste (Location Based Services, LBS)[50]. Sie bewegen sich technologisch an der Schnittstelle zwischen Geoinformationssystemen (GIS), Internetanwendungen und Mobilfunktechnologie. Diese Systeme ermittelt und vermitteln den Standort eines Geräts (mobiles Endgerät)[51]. Es fallen einerseits Daten an von (registrierten) Nutzerinnen und Nutzern des Services und andererseits Standortdaten von Geräten[52], die Personen zugeordnet werden können[53]. Die Angaben über die registrierten

44 Beispiele aus WEBER, E-Commerce und Recht, 470.
45 PROBST, Bestimmbarkeit, 1426 f.
46 ROSENTHAL, Art. 3 lit. a DSG N 40.
47 ROSENTHAL, Art. 3 lit. a DSG N 27.
48 In BGer 1P.51/2007 vom 24. September 2007, E. 3.5.4 hatte das Bundesgericht den Einsatz eines GPS-Peilsenders zur Ortung des Standortes eines Autos zu beurteilen.
49 BGer 1P.153/2005 vom 21. März 2005; 6B_275/2012 vom 26. Juli 2012, E. 1.4; 1B_348/2013 vom 21. Oktober 2013.
50 KETTIGER, Location Sharing Systeme, Rz 6; s.a. oben Rz 9.72 ff.
51 KETTIGER, Location Sharing Systeme, Rz 7.
52 Location Sharing Systeme können zu Navigationszwecken etwa Kartendaten der Landesvermessung oder andere Geobasisdaten verwenden.
53 KETTIGER, Location Sharing Systeme, Rz 11.

Nutzer stellen datenschutzrelevante Personendaten dar[54]. Das Wissen um den Standort des Geräts lässt aber grundsätzlich nicht bereits mit genügender Sicherheit auf konkrete Personen schliessen, die zu einem bestimmten Zeitpunkt das Gerät bedienen. Es wird wohl im Einzelfall zu entscheiden sein, ob die Person genügend bekannt ist oder gemacht werden kann.

2. Datenschutzrechtliche Sonderregelungen

a) Im Allgemeinen

Das *Datenschutzgesetz ist nicht anwendbar*, wenn Sachdaten keine Datenschutzrelevanz haben, oder *wenn andere Rechtsgrundlagen den Schutz der persönlichen Integrität* bereits garantieren. Es ist in diesem Sinn u.a.[55] nicht anwendbar auf Geodaten und Geobasisdaten ohne Datenschutzrelevanz, auf Personendaten, die zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gegeben werden, sowie auf Personendaten, bei denen eine Sonderregelung die Einhaltung des datenschutzrechtlichen Mindeststandards garantiert. **15.31**

Die Geodaten sind nicht zum persönlichen Gebrauch bestimmt oder beschränkt, sodass Art. 2 Abs. 2 lit. a DSG nicht angerufen werden kann. Ebenso wollen die gesetzlich normierten Geoinformationen (Geobasisdaten) für eine breite Nutzung zur Verfügung stehen (Art. 1 GeoIG). **15.32**

Auch die Sonderregelung für die Verwendung von Geobasisdaten in Prozessen und verwaltungsrechtlichen Verfahren (Art. 2 Abs. 2 lit. c DSG) treffen die Geobasisdaten nicht speziell, sind diese selber doch kaum Gegenstand solcher Verfahren. Immerhin sind im Prozess die Verfahrensregeln mit ihren Datenschutzbestimmungen zu beachten, wenn datenschutzrelevante Geobasisdaten als Beweisgrundlage verwendet werden. **15.33**

Vom Datenschutz geprägt sind hingegen die Regeln über das Bearbeiten von *Geobasisdaten in Registern und Katastern:* öffentliche Register des Privatrechts (unten Rz 15.35 ff.) und öffentliche Register des öffentlichen Rechts (unten Rz 15.38 ff.). **15.34**

b) Öffentliche Register des Privatrechts

15.35

54 BGE 136 II 508, 510 lehnt die Meinung von KETTIGER (Location Sharing Systeme, Rz 20) ab, dass IP-Adressen ausschliesslich in den Anwendungsbereich des Fernmeldegesetzes vom 30. April 1997 (FMG; SR 784.10) fallen. Das Bundesgericht bestätigte zwar, dass es sich bei den IP-Adressen um Adressierungselemente i.S.d. Fernmeldegesetzgebung handelt, hält aber zutreffend fest: „Das Fernmeldegeheimnis gilt jedoch von vornherein nur für denjenigen, der mit fernmeldedienstlichen Aufgaben 'betraut' ist (Art. 43 FMG; vgl. BGE 126 I 50 E. 6a S. 65 mit Hinweis)“ (BGE 136 II 508, 513 E. 3.1).

55 Zudem ist das DSG nicht anwendbar auf Beratungen in den eidgenössischen Räten und in den parlamentarischen Kommissionen (Art. 2 Abs. 2 lit. b DSG) und auf Personendaten, die das Internationale Komitee vom Roten Kreuz bearbeitet (Art. 2 Abs. 2 lit. e DSG)

Das Datenschutzgesetz ist nicht anwendbar auf *öffentliche Register des Privatrechtsverkehrs* (Art. 2 Abs. 2 lit. d DSG). Zu diesen Registern zählen das Grundbuch[56], das Zivilstandsregister, das Handelsregister, Register für Schuldbetreibung und Konkurs, Register für Eigentumsvorbehalte, Sortenschutz, gewerbliche Muster und Modelle sowie Fabrik- und Handelsmarken[57]. Der Datenschutz dieser Register ist in speziellen Gesetzen und Verordnungen detailliert geregelt.

15.36 Im Zusammenhang mit Geodaten und Geobasisdaten interessiert in erster Linie das Grundbuch. *Grundbuchdaten* haben einen Orts- und einen Rechtsbezug. Sie halten Informationen zu den Berechtigungen an bestimmten Liegenschaften fest, Berechtigungen, die sich aus dem ZGB ergeben. Nachdem das Grundeigentum gegenüber jedermann (erga omnes) wirkt, muss auch jedem bekannt sein, wo, wer, wann welche Berechtigungen hat oder hatte. Sowohl der Zweck der Publikation wie auch der Umfang sowie die Freiheiten und Schranken des Zugangs zu den Grundbuchdaten sind im Schweizerischen Zivilgesetzbuch (Art. 970 ZGB) und in der Grundbuchverordnung (Art. 26–34 BV) ausführlich geregelt und ersetzen die allgemeinen Bestimmungen des Datenschutzgesetzes.

15.37 Auch das *Vermessungswerk* ist ein öffentliches Register des Privatrechts, soweit es durch die Aufzeichnung des Grenzverlaufs die Liegenschaften individualisiert[58] und damit die Grundbuchführung erst ermöglicht[59]. Hier kommt nicht die Grundbuchregelung, sondern die im Geoinformationsgesetz vorgesehene Regelung über die öffentliche Auflage der Vermessungsergebnisse (Art. 32 Abs. 2 lit. b GeoIG[60]) zur Anwendung. Sie liefert eine genügende rechtliche Grundlage zur Veröffentlichung der Liegenschaftsgrenzen im Plan für das Grundbuch.

c) Öffentliche Register des öffentlichen Rechts

15.38 Das Datenschutzgesetz macht keinen Vorbehalt zu Gunsten von Bestimmungen über Daten in allgemein zugänglichen Registern des öffentlichen Rechts. Das *fachspezifische Bundesrecht*, das die raumwirksamen Tätigkeiten regelt, enthält aber umfassende Bestimmungen über den Inhalt und das Bearbeiten von Katastern, die ihre Grundlage im öffentlichen Recht finden, wie etwa Gefahrenkataster, Lärmschutzkataster, Altlastenkataster, aber auch Inventare über Hochmoore oder geschützte Gebäude[61]. Dieses fachspezifische Recht trägt dem Schutz der

56 Das Eidg. Amt für Grundbuch und Bodenrecht hat dies in den Erläuterungen vom 30. März 2005 im Zusammenhang mit der Änderung der Grundbuchverordnung vom 11. März 2005 ausdrücklich bestätigt.
57 Botschaft DSG 1988, 444.
58 HUSER, Vermessungsrecht, Rz 491ff.
59 HUSER, Geo-Informationsrecht, 175.
60 Es wird auf Art. 34 der Verordnung über die amtliche Vermessung (VAV), vom 18. November 1992 (SR 211.432.2) Bezug genommen, die ihrerseits wieder auf die Regelung des Zugangs nach Art. 10–13 GeoIG zurückverweist.
61 Dazu HUSER, Geo-Informationsrecht, S. 47ff.

Persönlichkeit Rechnung und geht als lex specialis dem Datenschutzrecht vor; für die kantonalen Geoinformationssysteme, die sich auf öffentliches Recht des Kantons stützen, entscheidet das kantonale Geoinformationsrecht.

15.39 Das Vermessungswerk enthält neben den Geobasisdaten über die Flächen der Grundstücke und (allenfalls) der beschränkten dinglichen Rechte[62] eine grosse Anzahl weiterer Geobasisdaten. Es sind v.a. *Georeferenzdaten*[63]. Sie liefern die geometrische Grundlage und den genauen Ortsbezug (auch) für die weiteren Geodaten und Geobasisdaten (Art. 3 lit. f GeoIG). Sie erscheinen meist in Kombination mit anderen Geodaten, die einen Bezug zu raumwirksamen Bestimmungen des öffentlichen Rechts haben. Diese Angaben werden gemäss den Sonderbestimmungen der jeweiligen Fachgesetzgebung (wie etwa RPG, USG, NHG i.V.m. dem GeoIG) verwaltet. Das Datenschutzgesetz kommt nur zur Anwendung, soweit das Fachgesetz oder das Geo-Informationsgesetz darauf verweist.

15.40 Geoinformationen aus verschiedenen Fachbereichen sind neuerdings im *Kataster der öffentlich-rechtlichen Eigentumsbeschränkungen* zusammengefasst (Art. 16–18 GeoIG, ÖREBKV[64]). Dieser Kataster wird – wie das Grundbuch – parzellenbezogen geführt, das heisst die Eigentumsbeschränkungen werden nach den betroffenen Liegenschaften geordnet[65]. Aus dem Kataster ergibt sich pro Liegenschaft die Information über Nutzungsbeschränkungen aus dem öffentlichen Recht. Der Inhalt des Katasters gilt als bekannt (Art. 17 GeoIG), die verwalteten Geobasisdaten müssen deshalb öffentlich zugänglich sein. Der Zugang erfolgt über einen Darstellungsdienst, d.h. „einen Internetdienst, mit dem darstellbare Geodatensätze angezeigt, vergrössert, verkleinert und verschoben, Daten überlagert und die für die Daten relevanten Inhalte von Geometadaten angezeigt werden können und der ein Navigieren in den Geodaten ermöglicht“ (Art. 2 lit. i GeoIV). – Zum Datenschutz finden sich in der ÖREB-Kataster-Verordnung keine Bestimmungen[66]. In diesen Kataster werden jedoch Geobasisdaten des Bundesrechts (und des kantonalen Rechts) verwaltet, deren Datenschutzrelevanz nach den Regeln des Geoinformationsgesetzes bereits geklärt ist, und die deshalb entsprechend aufbereitet sind.

3. Geodaten und öffentliches Recht

15.41 Im Recht der raumwirksamen Tätigkeiten finden sich Bestimmungen über die *Öffentlichkeit*

62 Dazu ausführlich MEINRAD HUSER, Darstellung von Grenzen zur Sicherung dinglicher Rechte, ZBGR 94/2013, 238 ff.
63 Beispiel öffentlicher Basisdaten (dazu unten 28.56 ff.).
64 Verordnung vom 2. September 2009 über den Kataster der öffentlich-rechtlichen Eigentumsbeschränkungen (SR 510.622.4).
65 Meinrad Huser, Publikation von Eigentumsbeschränkungen – neue Regeln, BR/DC 4/2010, 169 ff.
66 Auch DANIEL KETTIGER (Der Kataster der öffentlich-rechtlichen Eigentumsbeschränkungen, ZBGR 91/2010, 137 ff.) beschäftigt sich nicht mit dem Datenschutz.

mit und den Zugang zu staatlichen Geo-Informationen. Dabei steht der Anspruch auf Öffentlichkeit und Informationszugang der Allgemeinheit mit den berechtigten Datenschutzinteressen des Einzelnen in einem Spannungsverhältnis.

a) Das Öffentlichkeitsprinzip

15.42 Der Bedarf nach Geoinformationen hat sich mit der Entwicklung des raumwirksamen Rechts seit den sechziger Jahren des letzten Jahrhunderts gefestigt. Die Entwicklung führte zu einem *Systemwechsel beim Zugang* zu Dokumenten der staatlichen Verwaltungen[67].

15.43 Das Öffentlichkeitsprinzip[68] besagt, dass Informationen der Verwaltung grundsätzlich öffentlich zugänglich sind; der *Nichtzugang zu Dokumenten setzt eine ausdrückliche Regelung voraus*. Dieses Prinzip findet sich für die Bundesverwaltung im Bundesgesetz über die Öffentlichkeit (BGÖ), gilt aber – aufgrund eigener Regelungen – auch in vielen kantonalen Verwaltungen.

15.44 Das *Bundesgesetz über die Öffentlichkeit* stärkt den Anspruch auf Zugang zu den Daten der öffentlichen Verwaltung des Bundes, verdrängt aber den Datenschutz nicht. Die beiden Rechtsbereiche sind – auf Bundesebene – vielmehr koordiniert: So erlaubt das Datenschutzgesetz den Bundesorganen ausdrücklich, Personendaten bekanntzugeben, wenn die Daten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht (Art. 19 Abs. 1bis DSG). Personendaten dürfen zudem auch mittels Informations- und Kommunikationsdienste jedermann zugänglich gemacht werden, wenn eine Rechtsgrundlage die Veröffentlichung vorsieht (Art. 19 Abs. 3bis DSG). Das Öffentlichkeitsprinzip liefert also den Bundesorganen keinen Freipass für die Veröffentlichung von Personendaten, sondern unterzieht das Verhältnis zum Datenschutz einer Interessenabwägung[69].

b) Die Aarhus-Konvention

15.45 Das Übereinkommen über den Zugang zu Informationen, die Öffentlichkeitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten (Aarhus-Konvention[70]) will den *Zugang zu Umweltinformationen* verbessern[71]. Die Konvention statuiert einen weitgehenden Anspruch der Öffentlichkeit auf Zugang zu diesen Informationen (Art. 4). Bürgerinnen und Bürger sollen Dokumente bei Behörden mit Informationen im

67 Zur Entwicklung der Grundlagen und aus der Sicht des Journalismus: PETER STUDER, Das Öffentlichkeitsgesetz (BGÖ) ist heute ein Werkzeug für investigative Journalisten, Jusletter 11. Dezember 2013.

68 Unerheblich ist dabei, ob das Öffentlichkeitsprinzip in der Verfassung verankert ist oder im Gesetz. In vielen Kantonen wurde dieses Prinzip in der Verfassung eingeführt. Beim Bund steht es nicht auf Verfassungsstufe.

69 WALDMANN/BICKEL, § 12 N 99 f.

70 Botschaft Aarhus-Konvention, 4342.

71 Dazu BRUNNER/FLÜCKIGER, Rz 7; KETTIGER, Aarhus-Konvention, 789 ff.

Bereich Umwelt einsehen können. "Informationen über die Umwelt" sind sämtliche Informationen [...], die Auskunft geben über den Zustand von Umweltbestandteilen, über bestimmte Faktoren wie Stoffe, Energie, Lärm und Strahlung sowie den Zustand der menschlichen Gesundheit und Sicherheit, Bedingungen für menschliches Leben sowie Kulturstätten und Bauwerke soweit sie […] betroffen sind oder betroffen sein können."

15.46 Mit dem Öffentlichkeitsgesetz des Bundes ist ein *Einsichtsrecht* auf Bundesebene *in allgemeiner Weise* sichergestellt. Zudem wurden mit dem Bundesbeschluss über den Beitritt zur Aarhus-Konvention[72] die notwendigen Anpassungen im Umweltschutzgesetz gemacht.

15.47 Der Beitritt zur Konvention betrifft ebenso die Kantone. Auch sie haben den Zugang zu Umweltinformationen nach den Vorgaben der Konvention zu gewähren. Die meisten *Kantone* haben dies mit dem *Erlass eigener Regeln über die Öffentlichkeit* bereits vollzogen. Wo eine Regelung fehlt, setzt der neue Art. 10g Abs. 4 USG für die Geobasisdaten des Umweltrechts subsidiär anwendbares Recht: „Soweit die Kantone noch keine Bestimmungen über den Zugang zu Dokumenten erlassen haben, wenden sie die Bestimmungen dieses Gesetzes und des BGÖ sinngemäss an." Selbstverständlich gilt diese Ersatzlösung nicht nur bei fehlender, sondern auch bei ungenügender Lösung, wenn das kantonale Öffentlichkeitsgesetz den minimalen Zugang nach der Aarhus-Konvention nicht ermöglicht.

15.48 Die Entwicklung des einfachen und umfassenden Zugangs zu Umweltinformationen wird durch die *Rechtsprechung des europäischen Gerichtshofes* gestärkt. Dieser hat schon mehrmals eine Informationspflicht aus Art. 2 und 8 der EMRK abgeleitet[73].

c) Informationspflicht bei raumwirksamen Tätigkeiten

15.49 Die *Information* der Bevölkerung über die Planungsschritte ist eine *Grundpflicht der Raumplanung* (Art. 4 RPG[74]). Pläne im Bewilligungsverfahren sind öffentlich zugänglich. Das Gleiche gilt für das Verfahren der Umweltverträglichkeitsprüfungen[75]. Auch die Bearbeitung der Informationen über Altlasten, die ein Grundstück belasten und entwerten können[76], sowie weitere öffentlich-rechtlichen Eigentumsbeschränkungen sind allgemein zugängliche Geobasisdaten[77].

15.50 Zugang zu den Daten und eine Informationspflicht der Behörden bestehen aber nur innerhalb der *Schranken schutzwürdiger öffentlicher und privater Geheimhaltungsinteressen*[78]. Damit

---

72 Bundesbeschluss vom 27. September 2013 (BBl 2013 7403), in Kraft seit 1. Juni 2014.
73 Siehe die Hinweise bei BRUNNER/FLÜCKIGER, Rz 6–8.
74 Dazu WALDMANN/HÄNNI, Art. 4 RPG N 9 und 46 ff.
75 Siehe dazu die detaillierte Aufzählung in der Botschaft BGÖ, 1966. Ebenso WIESTNER, 41. ok.
76 Art. 21 Altlastenverordnung
77 Vgl. dazu die Angaben über die Öffentlichkeit von Geobasisdaten im Anhang zur GeoIV, etwa Identifikatoren 87 und 88, 96 und 97, 103 und 104, 116–118 sowie Anhang 1 zur GeoIV

stellt das Recht der raumwirksamen Tätigkeiten die Öffentlichkeitserfordernisse in einen sachgerechten Zusammenhang zum Datenschutz.

d) Geoinformationsgesetz

aa) Im Allgemeinen

15.51 Das Geoinformationsgesetz (GeoIG) ordnet aufgrund ausdrücklicher Verfassungskompetenzen (Art. 75a BV)[79] das Erheben, Bewirtschaften und Bekanntgeben[80] von Geobasisdaten[81]. Es bestimmt die Rahmenbedingungen und die Einzelheiten namentlich über den *Zugang und die Veröffentlichung der Geobasisdaten* im Internet. Es konkretisiert die Interessenabwägung (Art. 10 GeoIG) mit eigenen Bestimmungen und Verweisen auf das weitere Bundesrecht (Art. 11 GeoIG)[82].

15.52 Für *kantonale und kommunale* hoheitliche Tätigkeiten haben die Kantone eigene, aber auf die Bundesregelung abgestimmte *Vorschriften* erlassen (Art. 46 Abs. 4 GeoIG)[83].

bb) Datenschutz im Geoinformationsgesetz

15.53 Das Geoinformationsgesetz hat den *Zugang und die Nutzung von Geobasisdaten* des Bundesrechts in zwei Bestimmungen geregelt: Art. 10 GeoIG legt den Grundsatz fest, dass Geobasisdaten des Bundesrechts öffentlich zugänglich sind und von jeder Person genutzt werden können, sofern keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen. Art. 11 GeoIG regelt alsdann den Datenschutz, indem er einen Grossteil der Bestimmungen des eidgenössischen Datenschutzgesetzes auf Geobasisdaten des Bundesrechts für anwendbar erklärt.

15.54 Der Gesetzgeber hat also für Geobasisdaten des Bunderechts kein bereichsspezifisches Datenschutzrecht[84] geschaffen, sondern *Bestimmungen des eidgenössischen Datenschutzgesetzes* für *anwendbar* erklärt[85]. So sind Art. 1–11, 16–25, 27, 33, 36 und 37 DSG direkt anwendbar (Art. 11 GeoIG). Nur punktuell sieht das Geoinformationsgesetz eigene Schutzlösungen vor: So für die Pflichten der Nutzerinnen und Nutzer, namentlich hinsichtlich des Zugangs und des Datenschutzes bei der Weitergabe der Daten (Art. 12 Abs. 2

---

78 WALDMANN/HÄNNI, Art. 4 RPG N 12.

79 BELSER, § 5 N 37; ausführlich HUSER, Geo-Informationsrecht, 45 ff.

80 Das Geoinformationsrecht und sein umfassendes Verordnungsgeflecht bezwecken ausdrücklich, „dass Geodaten über das Gebiet der Schweiz den Behörden aller Stufen, wie auch der Wirtschaft der Gesellschaft und der Wissenschaft für eine breite Nutzung, nachhaltig, aktuell, rasch, einfach, in der erforderlichen Qualität und zu angemessenen Kosten zur Verfügung stehen“ (Art. 1 GeoIG).

81 Zum Begriff s. Art. 3 Abs. 1 lit. c GeoIG. Botschaft GeoIG, 7843 ff.; HUSER, Grundzüge, 151 f.

82 S.a. unten Rz 28.24

83 Zum Konflikt mit dem Datenschutzgesetz siehe Rz 15.111 ff.

84 S. dazu oben Rz 8.34 ff.

85 Siehe auch KETTIGER, URP, 775.

lit. c GeoIG, Art. 29 und 31 GeoIV), für den Austausch der Geobasisdaten unter den kantonalen und eidgenössischen Behörden (Art. 14 Abs. 1 und 2 GeoIG) sowie für die Auflage des Vermessungswerks nach Art. 32 Abs. 2 lit. d GeoIG.

Es ist zunächst nach Art. 2 Abs. 1 und Art. 3 lit. a DSG zu *prüfen, ob die Geobasisdaten* des Bundesrechts im Einzelfall oder in Kombination mit anderen Informationen *datenschutzrelevant sind*, weil sie grundsätzlich oder in einer bestimmten Verwendungsart Rückschlüsse auf konkrete Personen ermöglichen[86]. Trifft dies zu, kommen die Bestimmungen des Datenschutzgesetzes, auf die Art. 11 GeoIG verweist, direkt und umfassend zur Anwendung[87]; eine ergänzende Regelung findet sich im Geoinformationsgesetz – neben den erwähnten drei punktuellen Lösungen – nicht. **15.55**

Soweit die Prüfung nach Art. 2 Abs. 1 und Art. 3 lit. a DSG im Einzelfall zum Ergebnis führt, dass Geobasisdaten *keine Datenschutzrelevanz* haben, kommt das *Datenschutzgesetz generell nicht zur Anwendung*. Es gelten ausschliesslich die Vorschriften des Geoinformationsgesetzes über die Öffentlichkeit und den Zugang. Ein Blick in den Datenkatalog der Geobasisdaten des Bundesrechts (GeoIV – Anhang) zeigt, dass in der grossen Mehrheit reine Sachdaten geregelt sind, die nicht zu den datenschutzrelevanten Daten gehören. Immerhin stellen die Informationen aus dem Grundbuch (Grundeigentümer und dinglich Berechtigte) offensichtliche Personenangaben dar, deren Veröffentlichung im Zivilgesetzbuch aber ausdrücklich geregelt ist[88]. **15.56**

Aus der Zuweisung der Geobasisdaten des Bundesrechts zu einzelnen *Zugangskategorien im Anhang zur Geoinformationsverordnung* darf weder positiv noch negativ auf die Datenschutzrelevanz geschlossen werden. Die Erwähnung im Anhang zeigt nur, dass eine Geoinformation Teil eines Rechtssatzes ist und eine bestimmte Zugangsberechtigungsstufe erfüllt. Eine datenschutzrechtliche Wertung enthält sie nicht[89]. Der Anhang zur Geoinformationsverordnung teilt die Zugangsberechtigung nur für den Fall zu, dass die jeweiligen Geobasisdaten nicht nach den Regeln der Personendaten zu behandeln sind. **15.57**

4. Folgerungen für das anwendbare Recht

Es kann folgendes *Zwischenergebnis* festgehalten werden: 1. Geodaten (Ortsangaben ohne Rechtsbezug) werden in der Regel von Privaten erhoben und bearbeitet. Sie unterstehen dem Datenschutzgesetz des Bundes, wenn sie Rückschlüsse auf bestimmte und bestimmbare Personen i.S.d. Rechtsprechung zulassen. 2. Geobasisdaten (Daten mit Orts- und **15.58**

---

86 S. dazu oben Rz 15.7ff.

87 HUSER (Grundzüge, 155 f.) geht noch von einer analogen und ergänzenden Anwendung aus.

88 Siehe dazu Rz 15.123 ff.

89 Dazu HUSER, Grundzüge, 153 mit Hinweisen auf KETTIGER, Geheimhaltung und Öffentlichkeit, 59.

Rechtsbezug) werden von der öffentlichen Verwaltung bearbeitet und verwaltet. Sie unterstehen dem Geoinformationsgesetz und den wichtigsten Bearbeitungsgrundsätzen des Datenschutzgesetzes, wenn sie Rückschlüsse auf konkrete Personen ermöglichen. 3. Werden Geodaten oder Geobasisdaten mit weiteren Daten und Datenquellen verbunden, hat die Prüfung der Datenschutzrelevanz an diesem Produkt und nicht an den einzelnen Datenquellen anzusetzen. 4. Für Geobasisdaten ohne Datenschutzrelevanz kommen keine Datenschutzbestimmungen zur Anwendung, sondern Vorgaben über die Öffentlichkeit und den Zugang gemäss Geoinformationsgesetz. 5. Aufnahme- und Wiedergabegeräte sind Hilfsmittel für das Erheben und Bearbeiten von Personenangaben. Ihre technische Hilfe kann den Aufwand für Rückschlüsse auf konkrete Personen reduzieren und hat damit eine Bedeutung bei der Beurteilung der Datenschutzrelevanz. Der Datenschutz setzt aber richtigerweise bei den vermittelten Inhalten[90], und nicht bei den verwendeten Geräten an[91].

15.59 Die Frage der *Rechtmässigkeit*[92] *der Bearbeitung von Geodaten und Geobasisdaten* ist nach unterschiedlichen Rechtsgrundlagen zu beurteilen: Es stehen dazu die Datenschutzgesetze und die Geoinformationsgesetze je der verschiedenen Gebietskörperschaften (Bund, Kanton, Gemeinde) zur Verfügung. Theoretisch können auch Vorschriften in verwaltungsrechtlichen Fachgesetzen (USG, RPG) vorhanden sein, doch übernimmt das Geoinformationsgesetz in diesem Bereich die Koordination. Die gesetzlichen Grundlagen werden sinnvollerweise in zwei Kategorien getrennt behandelt: Geodaten (unten Rz 15.60 ff.) und Geobasisdaten (unten Rz 15.97 ff.).

III. Bearbeiten von Geodaten

1. Einleitung

15.60 Soweit datenschutzrelevante *Geodaten* bearbeitet werden, sind die *Regeln des Datenschutzgesetzes* und dabei namentlich die Bestimmungen über die Persönlichkeitsverletzungen (Art. 12 DSG) und die Rechtfertigungen (Art. 13 DSG) zu beachten. Diese Regeln kommen zum Tragen, wenn Private oder die öffentliche Verwaltung

90 In BGer 1P.51/2007 vom 24. September 2007, E. 3.5.4 beurteilte das Bundesgericht den Eingriff in die Freiheitsrechte (Intims- und Privatsphäre) beim Einsatz eines GPS-Peilsenders zur Ortung des Standortes eines Autos "(falls überhaupt ein solcher angenommen werden kann)" als sehr minim und mit den persönlichkeitsverletzenden Aufnahmen der Telefonabhörung, E-Mail-Überwachungen, Audio- oder Videoüberwachungen in Privaträumen nicht vergleichbar.

91 Das Bundesverwaltungsgericht hat diese Unterscheidung bei der Beurteilung des Einsatzes von Drohnen zur Grenzüberwachung nicht mit aller Konsequenz beachtet, wenn es zum Schluss kommt, der Einsatz von Bildaufnahme-, Bildaufzeichnungs- und anderen Überwachungs*geräten* unterständen dem Datenschutzgesetz (BVGer A-2484/2007 vom 26. Juni 2007, E. 2.2).

92 Grundlegend oben Rz 3.61 ff.

im Rahmen gewerblicher oder privatrechtlicher Tätigkeiten (Art. 23 DSG, Art. 19 GeoIG)[93] Geodaten bearbeiten. Die Vorschriften und das Vorgehen nach dem Datenschutzgesetz des Bundes finden auch Anwendung, wenn Private „behördliche" Geoinformationen mit Datenschutzrelevanz bearbeiten, die sie sich bei amtlichen Stellen des Bundes, der Kantone oder Gemeinden beschafft haben. Ob diese Daten während der Bearbeitungszeit durch die zuständige Verwaltungseinheit den Regeln des Geoinformationsgesetzes oder den besonderen Bestimmungen des Datenschutzgesetzes gemäss Art. 16 ff. DSG unterstanden haben, ist nicht von Bedeutung. Sobald Geobasisdaten im Privatbereich und nicht mehr aufgrund eines Rechtssatzes im öffentlichen Interesse bearbeitet werden, verlieren sie ihre hoheitliche Funktion. Es besteht kein Rechtsbezug mehr und es kommen weder die raumwirksamen Gesetze noch das Geoinformationsgesetz, sondern die Bestimmungen des eidgenössischen Datenschutzgesetzes über die Bearbeitung der Daten durch Private zur Anwendung[94].

2. Widerrechtliche Persönlichkeitsverletzung (Art. 12 DSG)

a) Im Allgemeinen

15.61 Wer Personendaten bearbeitet, darf die *Persönlichkeit nicht widerrechtlich verletzen* (Art. 12 Abs. 1 DSG). Er darf Personendaten insbesondere nicht entgegen den Grundsätzen des Datenschutzgesetzes bearbeiten, ohne Rechtfertigungsgrund Daten einer Person gegen deren ausdrücklichen Willen bearbeiten oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgeben (Art. 12 Abs. 2 DSG). Macht die betroffene Person die Daten allgemein zugänglich und untersagt sie die Bearbeitung nicht ausdrücklich, liegt regelmässig keine Persönlichkeitsverletzung vor (Art. 12 Abs. 3 DSG)[95].

15.62 Es ist zunächst zu klären, wann eine Persönlichkeitsverletzung vorliegt und welche Arten der Bearbeitungen widerrechtlich sind.

b) Persönlichkeitsverletzung

15.63 Zur Frage, ab wann das Bearbeiten von datenschutzrelevanten Geodaten die Persönlichkeit verletzt oder verletzen kann, finden sich in der Literatur und Rechtsprechung *unterschiedliche Aussagen*: Zum einen wird eine gewisse Intensität des Eingriffs in die Persönlichkeit verlangt[96]. Zum anderen wird die Veröffentlichung eines individualisierenden, d.h. nicht rein zufälligen Bildes ohne Einwilligung des Betroffenen immer als Persönlichkeitsverletzung

93 Bearbeitet eine Verwaltungsstelle Geoinformationen im Rahmen ihrer hoheitlichen Tätigkeit, braucht sie dazu eine gesetzliche Grundlage, womit diese Geodaten regelmässig unter die Definition der Geobasisdaten fallen.

94 Für Geobasisdaten der amtlichen Vermessung siehe Huser, Vermessungsrecht, Rz 688.

95 Siehe oben Rz 3.117 ff.

96 ROSENTHAL, Art. 12 DSG N 2.

angesehen[97]. Generell ist auf den Einzelfall abzustellen. Dabei ist die Sicht des Verletzenden ebenso einzubeziehen wie die Sicht des Opfers. Nicht das subjektive Empfinden ist zu beurteilen, sondern es ist ein objektiver Massstab anzuwenden[98]. Zu prüfen ist, „inwiefern die Umstände oder der Inhalt der betreffenden Datenbearbeitung bei objektiver Betrachtung als ernst zu nehmende Bedrohung oder Bestreitung des informationellen Selbstbestimmungsrechts […] oder anderer Persönlichkeitsgüter (z.B. Recht auf Achtung der geistigen Integrität, Geheim-, Intim- und Privatsphäre, Schutz der Ehre, Schutz der wirtschaftlichen Entfaltung […]) gelten müssen“[99].

15.64 *Mit Geodaten kombinierte Informationszusammenstellungen können die Persönlichkeit verletzen*, wenn sie datenschutzrelevant sind.. Jede Veröffentlichung einer Personendarstellung im Gelände oder in der heimischen Umgebung stellt eine Persönlichkeitsverletzung dar. Spezielle Umstände, wie etwa die Abbildung an sensiblen Orten, vor einem Altersheim, einem Spital oder andere Publikationen, die auf Schwächen einer Person hinweisen könnten, sind nicht nötig. Das Bundesgericht hat sich im Street-View-Entscheid mit dem Umfang der geschützten Umgebung ausführlich auseinandergesetzt und den Schutz des Menschen in der Umgebung weit gezogen. Nicht nur in Bereichen, die ausdrücklich vom öffentlichen Raum abgetrennt oder abgeschirmt sind, soll der Schutz des Privat- und Familienlebens gelten. Zum schützenswerten Privatbereich gehören vielmehr alle Bereiche, die Einblick ins Familienleben und in die Lebenssituation geben, seien sie geschützt oder offen: Wohnräume im Hausinnern, aber auch die Räumlichkeiten ausserhalb der Wohnmauern, wie etwa Gartensitzplätze und Freizeitbeschäftigungsanlagen[100]. Mit dieser Umschreibung wird eine grosse Anzahl Geodaten in den Bereich des Datenschutzes einbezogen.

15.65 Nicht nur die Bekanntgabe von Bildern mit Angaben über konkrete Personen verletzt die Persönlichkeit. Auch jede *unterbliebene Anonymisierung* eines Gesichtes oder eines anderen Identifikationsmerkmals (z.B. Haartracht, Körpergrösse, Sprache usw.) ist eine Persönlichkeitsverletzung, wenn bei der Veröffentlichung weiterhin die individualisierten Personen erkennbar bleiben.

c) Widerrechtlichkeit

15.66 Die Persönlichkeit ist dann verletzt, wenn die *Bearbeitung gegen die Grundsätze* nach Art. 4, nach Art. 5 Abs. 1 und nach Art. 7 DSG verstösst; auf die Intensivität der Verletzung kommt

97 Und zwar unabhängig davon, ob bereits die Aufnahme unrechtmässig erfolgte (BGE 138 II 346 E. 8.3).
98 BGer 5A_489/2012 vom 7. Dezember 2012, E. 2.3.
99 ROSENTHAL, Art. 12 DSG N 3.
100 Siehe dazu unten Rz 15.76.

es nicht an. Widerrechtlich ist das Bearbeiten von Daten auch, wenn verfassungsmässige Rechte (Persönlichkeitsschutz, weitere Geheimbereiche) missachtet werden.

aa) Verletzung des Datenschutzgesetzes

Nach Art. 12 Abs. 2 DSG gelten als *widerrechtliche Persönlichkeitsverletzungen* Verstösse gegen die Bearbeitungsgrundsätze (Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG), die Datenbearbeitung gegen den ausdrücklichen Willen der betroffenen Person oder die Bekanntgabe besonders schützenswerter Personendaten und Persönlichkeitsprofile. **15.67**

Beim Bearbeiten von Geodaten steht der *Verstoss gegen die Bearbeitungsgrundsätze* im Vordergrund: Personendaten dürfen nur rechtmässig bearbeitet werden (Art. 4 Abs. 1 DSG). Die Bearbeitung hat nach Treu und Glauben[101] zu erfolgen und muss verhältnismässig[102] sein (Art. 4 Abs. 2 DSG). Die Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Zweckbindung, Art. 4 Abs. 3 DSG). Schliesslich müssen das Beschaffen der Daten und deren Zweck für die betroffenen Personen erkennbar sein (Transparenz, Art. 4 Abs. 4 DSG). **15.68**

Es ist im Einzelfall zu klären, ob die erwähnten Voraussetzungen eingehalten sind. Insbesondere der *Schutz von Treu und Glauben* und die *Verhältnismässigkeit* können nicht nach allgemeinen Kriterien festgelegt sein, sondern stehen immer im Dienste der Einzelfallbeurteilung. Oft wird es bei der Bearbeitung von Geodaten aber nicht möglich sein, allen Betroffenen die Tatsache, dass Geodaten erfasst werden und welchen Zweck diese Datenbearbeitung verfolgt, mitzuteilen. Geodaten werden regelmässig grossflächig erhoben und aufgezeichnet. Die Wahrscheinlichkeit, dass dabei auch Personen oder deren Identifikationsmerkmale miterfasst werden, ist gross. Zwar werden sich die Gründe für das Erheben und Bearbeiten der Geobasisdaten aus der jeweiligen gesetzlichen Zweckbestimmung ergeben; für das Beschaffen von Geodaten, wie sie das Bundesgericht im Street-View Entscheid zu beurteilen hatte, bestand und besteht keine berechtigende Gesetzesgrundlage. Ebenso schwierig wird es sein, die Zweckbindung und die Transparenz für das Bearbeiten von Geodaten gegenüber den betroffenen Personen zu erklären. In Entscheid Street-View hat das Bundesgericht klargestellt, dass eine Beschriftung der Autos, mit denen die Strassenbilder aufgenommen wurden, dem Transparenzanliegen nicht genügen, auch wenn Street View in der Zwischenzeit bekannt sei und die Fahrten jeweils eine Woche vorher im Internet publik gemacht würden[103]. Bei Geodaten werden die **15.69**

---

[101] Dazu oben Rz 3.69 ff.
[102] Dazu oben Rz 3.75 ff.
103 BGE 138 II 346 E. 9.2

Bearbeitungsgrundsätze nach Art. 4 DSG aus reiner Überforderung der Datenbearbeiter regelmässig missachtet, womit sie eine Persönlichkeitsverletzung darstellen.

15.70 Wer datenschutzrelevante Geodaten bearbeitet, hat sich über deren *Richtigkeit* zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind (Art. 5 Abs. 1 DSG). Für Geodaten gilt diese Anforderung nicht nur im Hinblick auf den Persönlichkeitsschutz, sondern auch im Hinblick auf die richtige Darstellung der räumlichen Grundlagen.

15.71 *Zeitlich korrekte Informationen*[104] sind ein wichtiges Thema der Geodaten. Jede Information betrifft immer einen bestimmten Zeitpunkt. Geodaten und Darstellungen der Wirklichkeit wollen aktuell sein, sie wollen im Idealfall als Echtzeitbild dargestellt werden (Wetterkamera). Dieser Anspruch ist technisch kaum realisierbar. Aktualisierungen erfolgen regelmässig mit Verzögerungen[105]. Die jederzeitige Aktualität ist ausgeschlossen, wenn auf dem Bild bewegliche Informationen festgehalten sind; die zufällig abgebildete Person ist nur Minuten später nicht mehr am gleichen Ort. Unsicherheiten über die Aktualität sind zu verhindern, indem auf der Darstellung immer der Zeitpunkt der Aufnahme oder der Änderung angegeben wird[106]. Am zweckmässigsten ist die Löschung, sobald die Information nicht mehr aktuell ist und auch sonst nicht mehr gebraucht wird. Das Recht auf Vergessen[107] steht bisher bei der Bewirtschaftung von Geodaten nicht im Zentrum der Diskussionen[108], wird aber mit dem Entscheid des europäischen Gerichtshofs zur Möglichkeit, Links aus Datenschutzüberlegungen zu unterbinden[109], eine neue Bedeutung erhalten.

15.72 Die Datenbearbeitung ist schliesslich widerrechtlich, wenn Personendaten nicht durch *angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten* geschützt werden (Art. 7 DSG). Diese Voraussetzung ist zwingend für jedes Informationssystem, das eine verlässliche Informationsgrundlage sein will. Es ist im Einzelfall zu beurteilen, ob diese Voraussetzungen eingehalten sind[110].

bb) Verletzung von Grundrechten

15.73

---

104 HUSER, Geo-Informationsrecht, 142.

105 Dazu auch BSK DSG-MAURER-LAMBROU/SCHÖNBÄCHLER, Art. 5 N 7.

106 Mit einem solchen Hinweis kann eine allfällige Nicht-Anpassung gerechtfertigt werden (Art. 5 Abs. 2 DSG). Zum Berichtigungsanspruch siehe BSK DSG – Maurer-Lambrou/Schönbächler, Art. 5 N 14ff.

107 Siehe die Übersicht bei ROSENTHAL, Art. 13 DSG N 22.

108 Kritisch zur Veränderung der Datenschutzrelevanz infolge Zeitablaufs Huser, Geo-Informationsrecht, 172.

109 Siehe dazu oben Rz 15.24 f.

110 Art. 14 GeoIV setzt diesen Stand auch bei Geobasisdaten voraus, deren Bearbeitung nicht nach dem Datenschutzgesetz zu beurteilen ist.

Widerrechtlich sind *Massnahmen, die gegen verfassungsmässige Rechte* verstossen. Die Wahrung der Grundrechte richtet sich zwar in erster Linie an den Staat. Die Behörden haben aber dafür zu sorgen, dass die Grundrechte auch unter Privaten wirksam werden (Art. 35 Abs. 3 BV)[111]. „Der Verwirklichung dieses verfassungsrechtlichen Auftrags dient im vorliegenden Zusammenhang unter anderem das Tätigwerden des EDÖB gemäss Art. 29 DSG […]“[112]. Die Grundsätze, die das Bundesgericht aus diesen Interventionen, aber auch aus subsidiären Verfassungsbeschwerden (Art. 116 BGG) direkt aus den Grundrechten herleitet, bereichern die Praxis und dienen der Auslegung des Datenschutzgesetzes.

15.74 *Das Bearbeiten von Personendaten ist* grundrechtlich *doppelt eingeschränkt*[113]: Durch den Schutz des Privat- und Familienlebens (Art. 13 Abs. 1 BV) und durch den Schutz vor Missbrauch der persönlichen Daten (Art. 13 Abs. 2 BV). Werden diese Schranken durchbrochen, besteht eine widerrechtliche Datenbearbeitung und damit eine Persönlichkeitsverletzung. Der Doppelbegriff Privat- und Familienleben umfasst alle Lebenssachverhalte, die mit der Persönlichkeit des Menschen verbunden sind. Sie können aus diesem Grund nur fallbezogen beurteilt werden. Generell gilt: „Äusserungen und Handlungen fallen nicht unter den Schutzbereich des Privatlebens, wenn sie öffentlich erkenn- oder einsehbar sind und kein Interesse an ihrer Geheimhaltung oder Vertraulichkeit besteht“[114].

15.75 Die neuere Rechtsprechung hat sich vor allem mit den Missbräuchen im Sozialversicherungswesen befasst. Dabei legte sie auch Grundsätze fest, wie weit die Privatsphäre geschützt sei. Das Bundesgericht stellte zunächst klar, dass die *Überwachung von Personen durch private Detektive ein Eingriff in die grundrechtliche Position* sei. So lange die Observation aber im öffentlichen Raum stattfinde, sei der Eingriff als geringfügig zu bezeichnen[115]. Beobachtungen in einem frei einsehbaren privaten Raum – gefilmt wurden Tätigkeiten auf einem Balkon, der gegen Einblicke nicht besonders geschützt war – wurde als Verletzung der Privatsphäre und Einschränkung des verfassungsrechtlichen Persönlichkeitsschutzes gewertet[116].

15.76 Mit dem *Entscheid „Street-View“* unterstellt das Bundesgericht – wie gesehen[117] - weite Bereiche der bewohnten Umgebung dem Schutz des Privat- und Familienlebens. Dieses weite Verständnis des privaten Schutzbereichs ohne Rücksicht auf den Willen des Geschützten ist

111 Dazu WEBER/HEINRICH, 491 ff.
112 BGE 138 II 346 E. 8.2
113 Siehe dazu auch oben Rz 2.2 ff.
114 BREITENMOSER, Art. 13 BV N 12. Zur Observation im frei einsehbaren Raum s.a. unten Rz 17.61 f.
115 BGE 135 I 169
116 BGE 137 I 330 f. E. 5; s.a. unten Rz 17.61 ff.
117 Siehe dazu oben Rz 15. 64. Im Fall des Zürcher Polizeigesetzes hatte das Bundesgericht ähnlich argumentiert: „Somit kann die Überwachung gemäss § 32 PolG uneingeschränkt allgemein zugängliche Orte erfassen, mithin den gesamten öffentlichen Raum auf dem gesamten Kantonsgebiet, ohne dass irgendwelche Einschränkungen, Präzisierungen oder Schwerpunkte zum Ausdruck kämen“ (BGE 136 I 87 E. 8).

abzulehnen[118]. Die Zugänglichkeit zur Privatsphäre kann nicht allein objektiv festgelegt werden, sondern muss sich auch am Willen des Grundeigentümers orientieren. Entscheidend muss auch sein, wie der Interessierte (Grundeigentümer, dinglich Berechtigter) für sich den Schutzbereich definiert und der Allgemeinheit auch kenntlich macht (Zäune, Mauern, Bepflanzungen, Abdeckungen usw.). Bezeichnet er den geschützten Raum nicht, darf davon ausgegangen werden, dass die Sicht auf den Gartensitzplatz nicht verboten ist. Müssen aber für die Sicht auf den privaten Bereich Leitern oder spezielle Aufnahmegeräte verwendet werden, weil sich die Privatperson bewusst durch Schutzmassnahmen der öffentlichen Einsicht entziehen will, ist die Quelle nicht mehr allgemein zugänglich.

cc) Verletzung weiterer Geheimbereiche

15.77 Geodaten unterliegen nicht nur den *Schranken* aus dem Persönlichkeitsschutz, sondern auch *aus weiteren Geheimbereichen*. Zu erwähnen sind das Unternehmensgeheimnis, das Berufsgeheimnis, das Amtsgeheimnis und v.a. auch die militärischen Geheimnisse[119].

15.78 Diese Geheimbereiche *schützen nicht die Privatsphäre* oder die Persönlichkeit an sich. Im Zusammenhang mit dem Datenschutz muss darauf aber nicht näher eingegangen werden.

3. Rechtfertigungsgründe

15.79 Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (Art. 13 Abs. 1 DSG, ebenso Art. 28 Abs. 1 ZGB)[120]. Eine *Persönlichkeitsverletzung ist also rechtmässig,* wenn das Datenschutzgesetz dies zulässt, wenn der Verletzte eingewilligt hat oder wenn ein überwiegendes privates oder öffentliches Interesse vorliegt.

a) Rechtfertigungsgründe des Datenschutzgesetzes (Art. 13 DSG)

aa) Im Allgemeinen

15.80 Das Datenschutzgesetz zählt *Rechtfertigungsgründe* auf, die *direkt anwendbar* sind: Rechtfertigung durch Gesetze, durch Einwilligung des oder der Verletzten oder durch ein überwiegendes privates oder öffentliches Interesse.

15.81

---

118 Auch ROSENTHAL (Entwicklungen, 723) sieht im Street-View-Bundesgerichtsentscheid die zur Observation im Sozialversicherungsbereich entwickelte Sphärentheorie in Frage gestellt.

119 Einzelheiten über den Zusammenhang mit Geobasisdaten siehe HUSER, Geo-Informationsrecht, 174 ff.

120 S.a. oben Rz 3.123 ff.

Es enthält insbesondere einen *zweckgerichteten Katalog von Rechtfertigungsgründen*, die bei einem überwiegenden Interesse zulässig sind (Art. 13 Abs. 2 DSG). Ob eine konkrete Persönlichkeitsverletzung vorliegt, die sich rechtfertigen lässt und deshalb zu dulden ist, muss im Einzelfall anhand dieser beispielhaft aufgezählten Gründe geklärt werden.

bb) Einwilligung der Verletzten

15.82 Eine Persönlichkeitsverletzung ist nicht widerrechtlich, wenn die betroffene Person der Datenbearbeitung zustimmt (Art. 13 Abs. 1 DSG)[121]. Die *Zustimmung* muss *für die konkrete Datenbearbeitung* erfolgen und freiwillig sein. Die Einwilligung kann jede Persönlichkeitsverletzung rechtfertigen, auch Verstösse gegen die allgemeinen Grundsätze der Datenbearbeitung. „Je sensibler die in Frage stehenden Personendaten sind, je schwerer die drohende Persönlichkeitsverletzung, desto höhere Anforderungen sind an die Einwilligung zu stellen“[122].

15.83 Beim Fotografieren von Strassenzügen oder Abbilden ganzer Landschaften werden auch *zufällig anwesende Personen* Teil des Bildes. Diese Personen müssten der Veröffentlichung zustimmen, wenn die Bekanntgabe der Aufnahmen rechtmässig sein soll. Im Falle Street-View wurde die Öffentlichkeit aber nur auf der Webseite über die bevorstehenden Aufnahmen mit den mit Kameras ausgerüsteten Fahrzeugen aufmerksam gemacht. Es liegt auf der Hand, dass kaum jemand sich bewusst war, dass er oder sie demnächst in den Fokus einer Kamera geraten könnte. Viele Personen dürften die Beschaffung ihrer Personendaten selbst dann nicht realisiert haben, als sie die Aufnahmefahrzeuge in den Strassen wahrnahmen. Eine Einwilligung der Verletzten (Art. 4 Abs. 5 DSG) lag jedenfalls nicht vor und ist bei den flächendeckenden Fahrten kaum möglich oder nur mit so grossem Aufwand verbunden, dass Private dies gar nicht realisieren können.

15.84 Das Bundesgericht hat beim Street-View-Entscheid die Schwierigkeiten der vorgängigen Einwilligung aller zufällig anwesenden Personen erkannt. Es hat deshalb im Rahmen einer gesamthaften Güterabwägung an Stelle der Einwilligung aller Betroffenen unter strengen Voraussetzungen die Form eines *Widerspruchsrechts* akzeptiert. Dieses Vorgehen sei – so die Begründung im konkreten Fall – vertretbar, nachdem ein stark überwiegender Teil der Bilder vor der Publikation im Internet automatisch korrekt anonymisiert worden war. Das Bundesgericht hält jedoch ausdrücklich fest, dass im Rahmen der Güterabwägung nur eine kleine Fehlerquote von 1 % bei der automatischen Anonymisierung hingenommen werden könne und die Betreiberin verpflichtet sei, mit allen ihr zur Verfügung stehenden Mitteln eine

---

[121] Grundlegend oben Rz 3.64 ff. und Rz 3.128 ff.

[122] BSK DSG-RAMPINI, Art. 13 N 3.

vollständige Anonymisierung anzustreben sowie die automatische Anonymisierung laufend dem Stand der Technik anzupassen. Es verlangt zudem klare Hinweise für den Betrachter auf die Anonymisierungsmöglichkeiten. Eine kleine Schaltfläche („ein Problem melden“) genüge jedenfalls nicht. Den Benutzern müsse vielmehr ein gut sichtbarer Link – etwa mit dem klaren Hinweis „Anonymisierung verlangen“ – zur Verfügung stehen. Aus diesem Hinweis müsse sich klar ergeben, dass die Benutzer die Anonymisierung unzulässiger Inhalte veranlassen können. Gesuche müssen alsdann rasch, kostenlos und ohne Interessennachweis, also unbürokratisch, umgesetzt werden[123].

cc) Überwiegendes privates (und öffentliches) Interesse

15.85 Art. 13 Abs. 2 DSG zählt *Interessenlagen* auf, *die eine Verletzung der Persönlichkeit rechtfertigen* und daher datenschutzrechtlich zulässig sind. Das ist der Fall, wenn in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über den Vertragspartner bearbeitet werden (lit. a); wenn Daten über Wettbewerbskonkurrenten bearbeitet werden, ohne diese Dritten bekanntzugeben (lit. b); wenn Personendaten zur Prüfung der Kreditwürdigkeit bearbeitet werden (besonders schützenswerte Personendaten und Persönlichkeitsprofile ausgenommen, lit. c); wenn beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet werden (lit. d); wenn Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet werden (lit. e) und wenn Daten über eine Person des öffentlichen Lebens gesammelt werden, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen (lit. f). Die Aufzählung ist beispielhaft und nicht abschliessend.

15.86 Beim Bearbeiten von Geodaten steht der Rechtfertigungsgrund nach Art. 13 Abs. 2 lit. e DSG im Vordergrund. Ein überwiegendes Interesse an der Bearbeitung datenschutzrelevanter Daten ist unter zwei Voraussetzungen gegeben: Der *Zweck der Bearbeitung* darf *nicht personenbezogen* sein[124], und die betroffenen *Personen* dürfen *nicht bestimmbar* sein, wenn die Ergebnisse der Datenbearbeitung veröffentlich werden[125]. Als Veröffentlichung gilt nicht erst die Publikation in einem Medium, sondern bereits wenn die Bearbeitungsergebnisse auch ausserhalb eines Kreises bekannt gemacht werden, der zur Vertraulichkeit bezüglich der Personendaten verpflichtet ist[126].

15.87

123 BGE 138 II 346 E. 10.6.3
124 ROSENTHAL, Art. 13 DSG N 60.
125 ROSENTHAL, Art. 13 DSG N 62.
126 ROSENTHAL, Art. 13 DSG N 63.

Geodaten fallen typischerweise *bei der Raumplanungen* an; dabei stehen nicht der Mensch als Individuum, sondern die Topographie, Bodengestaltung und die bereits vorhandenen Infrastrukturanlagen im Mittelpunkt. Falls bei diesen Tätigkeiten trotzdem Personendaten anfallen, handelt es sich lediglich um einen unbeabsichtigten Nebeneffekt, da der Zweck nicht auf das Bearbeiten von Personendaten gerichtet ist. Solange solche Aufnahmen zudem nur für die internen Planungsarbeiten verwendet werden, liegt allenfalls keine Veröffentlichung vor. Werden aber solche Ergebnisse etwa in parlamentarischen Kommissionen oder zur Illustration in Abstimmungsbroschüren verwendet, müssen abgebildete Personen – so weit möglich – anonymisiert bzw. abgedeckt werden[127].

15.88 Auf den Rechtsfertigungsgrund nach Art. 13 Abs. 2 lit. e DSG können sich etwa Hochschulen berufen, soweit sie für Geländeaufnahmen im schulischen Bereich Drohnen einsetzen. Um *Bilder für die Forschung* zu nutzen oder den Drohnenbetrieb auch für die Ausbildung einzusetzen, kann die Datenbearbeitung – nebenbei – auch Personendaten enthalten. Dies ist gerechtfertigt, solange die Geodaten im engen schulischen Umfeld genutzt werden. Trifft dies nicht zu, müssen die Informationen oder Darstellungen bestmöglich anonymisiert werden. Dieses Ergebnis deckt sich letztlich mit den Ausführungen des Bundesgerichts zu den Street-View-Aufnahmen[128].

b) Rechtfertigung durch andere gesetzliche Grundlagen

15.89 Wie gesehen[129] besteht im Recht der raumwirksamen Tätigkeiten oft die Pflicht zur Veröffentlichung. Soweit diese *Pflichten in einem Gesetz* im formellen Sinn enthalten sind, können sie eine allfällige Verletzung von Persönlichkeitsrechten rechtfertigen. Es ist dabei im Einzelfall zu klären, ob der Umfang der Publikation dem Zweck des Sachgesetzes entspricht. Ist dies nicht der Fall, wäre das Fachgesetz verletzt, und eine Rechtfertigung wäre ohne diese Rechtsgrundlage nicht gegeben.

15.90 Das Geoinformationsgesetz enthält keine Bestimmungen über das Bearbeiten von Geodaten; es stellt die rechtlichen Rahmenbedingungen nur für die Geobasisdaten zur Verfügung. Soweit *Geodaten* datenschutzrelevant sind, kommen die *Rechtfertigungsgründe des Datenschutzgesetzes* zur Anwendung (Art. 12 und 13 DSG).

15.91 Das Bundesgericht anerkennt eine *gesetzliche Rechtfertigung für persönlichkeitsverletzende Aufnahmen* im Rahmen der Kontrolle von Sozialhilfebezüger in der Abklärungspflicht des Versicherungsträgers in Art. 43 ATSG und der Auskunftspflicht des Versicherungsnehmers in

127 ROSENTHAL, Art. 13 DSG N 65.
128 BGE 138 II 364 f. E. 10.3. und 10.6.
129 Dazu oben Rz 15.41 ff.

Art. 28 Abs. 2 ATSG[130]. Eine regelmässige Observation versicherter Personen durch Privatdetektive stelle ein relativ geringfügiger Eingriff in die grundrechtlichen Positionen der überwachten Personen dar, wenn sie sich auf den öffentlichen Raum beschränke[131]. Das öffentliche Interesse an der Einschränkung des Schutzes der Privatsphäre liege darin, keine nicht geschuldeten Leistungen zu erbringen, um die Gemeinschaft der Versicherten nicht zu schädigen[132]. Und die Anordnung einer Observation durch einen Privatdetektiv sei zur Erreichung des angestrebten Zieles (wirksame Bekämpfung von Missbräuchen) geeignet und erforderlich, da nur diese Beweismittel – beispielsweise bei offensichtlichen Anhaltspunkten einer effektiv bestehenden Arbeitsfähigkeit – eine unmittelbare Wahrnehmung wiedergeben können[133]. Der Eingriff sei deshalb auch verhältnismässig.

15.92 Die Street-View-Aufnahmen sind Geodaten und haben nicht nur *keine Grundlage in einem Rechtssatz* im Zusammenhang mit raumwirksamen Tätigkeiten, sondern auch keine spezifischen rechtlichen Rahmenbedingungen, die die Einhaltung der Grundrechte und Gesetze garantieren könnten; es fehlt ihnen insbesondere ein gesetzlicher Rechtfertigungsgrund. Das Bundesgericht erachtete deshalb den Persönlichkeitsschutz als verletzt und die widerrechtlichen Darstellungen mussten grundsätzlich beseitigt, sprich anonymisiert werden[134].

c) Interessenabwägung

15.93 Bei der Beurteilung der Rechtmässigkeit einer Persönlichkeitsverletzung ist eine *Güterabwägung* vorzunehmen. Es sind die auf dem Spiel stehenden Interessen gegeneinander abzuwägen[135] und es ist auch zu prüfen, ob sowohl die Ziele, die der Urheber einer Persönlichkeitsverletzung verfolgt, als auch die Mittel, derer er sich bedient, schutzwürdig sind[136]. In diesem Rahmen sind bei der Anwendung von Art. 28 ZGB (bzw. Art. 12 DSG) auch die Grundrechte[137] zu berücksichtigen[138].

15.94 Bei dieser Abwägung zieht das Bundesgericht regelmässig auch die im Spiel stehenden *wirtschaftlichen Interessen* bei: So wurden die Anliegen, eine Datenbearbeitung möglichst effizient zu gestalten oder die eigenen Geschäftsabläufe zu optimieren ausdrücklich als schützenswerte Interessen bezeichnet. Im Entscheid Logistep AG hat es das wirtschaftliche

130 BGE 135 I 173 E. 5.4; zur Datenbearbeitung im Sozialversicherungswesen s. oben Rz 3.45 und 13.13 ff.; über Massnahmen zur Verhinderung des Versichungsmissbrauchs s. oben Rz 13.165 ff.
131 BGE 135 I 174 E. 5.4.2.
132 BGE 135 I 174 E. 5.5.
133 BGE 135 I 174 f. E. 5.6.
134 BGE 138 II 346, 362 E. 7.2..
135 WEBER/HEINRICH, 487 f.
136 BGE 126 III 305, 306 E. 4a.
137 WEBER/HEINRICH (486 f.) leiten aus dem Street-View-Entscheid des Bundesgerichts einen Vorrang des Persönlichkeitsrechts ab.
138 BGer 5A_489/2012 vom 7. Dezember 2012, E. 2.4.

Interesse an der Suche nach urheberrechtlich geschützten Werken im Internet mit einer eigens dafür entwickelten Software nicht als genügend wichtig erachtet, um Persönlichkeitsverletzungen zu rechtfertigen. Grundlegend für diesen Entscheid waren v.a. die Unsicherheit der Methode, insbesondere die Unklarheit in Bezug auf die Speicherung und die mögliche Verwendung der Daten ausserhalb eines ordentlichen Gerichtsverfahrens[139]. Im Entscheid Street-View hat das Bundesgericht wirtschaftliche Interessen insofern berücksichtigt, als bereits bestehende Fotoaufnahmen nicht zu hundert Prozent anonymisiert werden mussten[140].

15.95 Im Entscheid Street-View hat das Bundesgericht aus der *Entwicklung sozialer Aspekte* zudem gefolgert: „Bei einer gesamthaften Abwägung der verschiedenen Interessen ist auch zu beachten, dass angesichts der in der heutigen Gesellschaft faktisch bestehenden Einbindung von Personendaten in die soziale Realität nicht ein totaler Schutz vor einer unbefugten Bildveröffentlichung gewährleistet werden kann. Häufig haben die Bilder und betroffenen Daten nur eine geringe Persönlichkeitsrelevanz …“ Es sei davon auszugehen, dass „ein namhafter Teil der mit Street View hervorgerufenen Persönlichkeitsverletzungen nicht sehr schwer wiegt und mit einer unbürokratisch gehandhabten Widerspruchsmöglichkeit hinreichend korrigiert werden kann […]“[141].

15.96 Auch das „*Informationsinteresse des Publikums*“ kann bei der Interessenabwägung eine bedeutende Rolle spielen. Zwar hat das Bundesgericht die Frage, ob dieses Interesse unter das Grundrecht der Informationsfreiheit falle, ausdrücklich nicht beantwortet[142], bei der Prüfung der Rechtfertigung nach Art. 13 DSG jedoch einbezogen. Es macht richtigerweise Sinn, die „Interessen des Publikums“ als Summe der Interessen der einzelnen Informationsberechtigten zu begreifen und diesen Anspruch auf das Grundrecht der Meinungs- und Informationsfreiheit abzustützen.

IV. Bearbeiten von Geobasisdaten

1. Einleitung

15.97 Geobasisdaten (Art. 3 Abs. 1 lit. c GeoIG) werden durch die öffentliche Verwaltung[143] erarbeitet und bewirtschaftet. Die *Frage des Datenschutzes bei Geobasisdaten* stellt sich deshalb nur *für die* Bundesbehörden sowie die kantonalen und kommunalen Behörden. Es

139 BGE 136 II 524.
140 BGE 138 II 364 f. E. 10.3.
141 BGE 138 II 372 E. 10.6.6.
142 BGE 138 II 366 f. E. 10.6.1.
143 Durch eigene Angestellte oder durch von ihnen Beauftragte.

stehen sich nicht Interessen zwischen zwei Privaten gegenüber, sondern das öffentliche Interesse an der Bearbeitung der Daten zur Erfüllung des staatlichen Auftrags gegen ein allfälliges Schutzinteresse Privater. Das Bewirtschaften von datenschutzrelevanten Geobasisdaten durch Behörden wird deshalb durch das Geoinformationsrecht geregelt, das in Art. 11 GeoIG namentlich auch auf den vierten Abschnitt des Datenschutzgesetzes (Art. 16 ff. GeoIG) verweist.

15.98 Sind Geobasisdaten *Sachdaten ohne Datenschutzrelevanz*, d.h. keine Personendaten i.S.d. DSG, untersteht ihre Bearbeitung ausschliesslich dem Privatrecht oder dem öffentlichen Recht. Das Datenschutzrecht jedenfalls findet in diesen Fällen keine Anwendung.

2. Bearbeiten nach dem Datenschutzrecht

a) Bearbeiten durch Private

15.99 Nutzerinnen und Nutzer ohne hoheitliche Aufgaben können Geoinformationen, die als Geobasisdaten erstellt wurden, im Privatbereich nutzen. Die Geobasisdaten verlieren in diesen Fällen den hoheitlichen Status. Das Geoinformationsgesetz kommt nicht mehr zur Anwendung[144].

15.100 Die Weiterverwendung von Geobasisdaten durch Private und namentlich die Kombination mit personenrelevanten Daten und Datenquellen richten sich direkt – und nicht aufgrund des Verweises in Art. 11 GeoIG – nach dem *eidgenössischen Datenschutzgesetz*[145]. Dies wird mit dem Hinweis in Art. 29 GeoIV auf die datenschutzrechtliche Verantwortung der Nutzerinnen und Nutzern verdeutlicht[146].

b) Bearbeiten durch Behörden

aa) Legalitätsprinzip

15.101 Staatliches Handeln ist immer auf eine gesetzliche Grundlage angewiesen (Legalitätsprinzip). Ob Geobasisdaten als Personendaten, als Datenquelle eines Kombinationsprodukts oder als reine Sachdaten gelten, ist unter dem Aspekt des Legalitätsprinzips nicht entscheidend. Behörden und Angestellte der Gemeinde, des Kantons oder des Bundes dürfen Geoinformationen nicht nach freiem Ermessen erwerben, bearbeiten und benutzen.

---

144 Siehe Rz 15.56 ff.; ebenso HUSER, Vermessungsrecht, Rz 643 ff. Das GeoIG ist konsequent, indem es den Privaten für die Nutzung von staatlichen Stellen bezogener Geodaten auch gegenüber dem eidgenössischen Öffentlichkeits- und Datenschutzbeauftragten verantwortlich macht (Art. 29 GeoIV) und bei der Nutzung dieser Geobasisdaten im gewerblichen Rahmen richtigerweise von Geodaten spricht (Art. 19 GeoIG).

145 Siehe dazu ROSENTHAL/JÖHRI, Art. 2 DSG N 50.

146 Verantwortlich i.S.d. Datenschutzgesetzes ist derjenige, der über den Zweck und den Inhalt einer Datensammlung entscheidet (ROSENTHAL, Art. 3 lit. i DSG N 105 ff.); zur Datenherrschaft s.a. Huser, Geo-Informationsrecht, 82ff. sowie unten Rz 28.49 ff.

Erforderlich ist immer eine *gesetzliche Grundlage*[147], die sich auf ein *öffentliches Interesse*[148] stützt und die Schranken der Verfassung einhält[149].

15.102 Der Bund, die Kantone und Gemeinden setzen die moderne Technik beim Erheben oder Bearbeiten von Geobasisdaten ein. So lassen das Bundesamt für Landestopographie, aber auch einzelne Kantone, für die Erstellung von Landeskarten oder als Grundlage der amtlichen Vermessung Flugaufnahmen machen. Diese Orthofotos sind mit Aufnahmen Privater aus Flugzeugen identisch, teilweise sogar genauer. Für den Strassenunterhalt oder für Leitungskataster werden Strassenzüge durch Drohnen, also nach ähnlichen Methoden gefilmt, wie sie beim Street-View-Entscheid aus datenschutzrechtlicher Sicht kritisch hinterfragt wurden. All diese Aufnahmen durch staatliche Stellen müssen dem Legalitätsprinzip genügen, also eine *genügende gesetzliche Grundlage* haben. Auf Bundesebene übernimmt das Geoinformationsgesetz diese Funktion. Auf kantonaler und kommunaler Stufe sind analoge Regelungen festzulegen, wenn die Aufnahmen rechtmässig sein wollen[150].

bb) Bearbeiten durch Verwaltungseinheiten des Bundes

15.103 Das Datenschutzgesetz enthält *spezielle Regelungen über das Bearbeiten von Daten durch Bundesorgane* (Art. 16–25bis DSG), die auch für die datenschutzrelevanten Geobasisdaten des Bundesrechts gelten.

15.104 Solche Geobasisdaten dürfen nur bearbeitet werden, wenn dafür eine gesetzliche Grundlage besteht (Art. 17 DSG). Handelt es sich nicht um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, genügt eine Grundlage in einem Gesetz im materiellen Sinn[151]. Mit dem Geoinformationsgesetz und den weiteren Gesetzen über die raumwirksamen Tätigkeiten bestehen die erforderlichen Grundlagen. Für den Datenschutz verweisen diese Grundlagen explizit auf das Datenschutzgesetz und dabei v.a. auf den vierten Abschnitt über das Bearbeiten von Personendaten durch Bundesorgane (Art. 11 GeoIG). Von besonderer Bedeutung für die Geobasisdaten mit Datenschutzrelevanz sind die Bestimmungen über das Bekanntgeben (Art. 19 DSG), das Sperrrecht (Art. 20 DSG[152]) sowie das Bearbeiten für Forschung, Planung und Statistik (Art. 22 DSG). Ob das flächendeckende Erheben

147 Dazu auch JÖHRI, Art. 17 DSG N 2 ff.

148 Siehe die Begründung bei HUSER, Grundzüge, 144 f.

149 Verfassungswidrige Rechtsetzung kann das Bundesgericht aus Gründen der Gewaltenteilung nicht feststellen. Doch darf die (negative) Beurteilung des allgemein gehaltenen Paragrafen im Polizeigesetz des Kantons Zürich (BGE 136 I 87 E. 8) auch als Richtschnur für den Gesetzgebungsfreiraum des Bundes verstanden werden.

150 Eine gesetzliche Grundlage ist v.a. dann zwingend, wenn besonders schützenswerte Personendaten (Art. 3 lit. c DSG) oder Persönlichkeitsprofile (Art. 3 lit. d DSG) bewirtschaftet werden (BSK DSG-BALLENEGGER, Art. 17 N 4 ff.) oder wenn die erhobenen Informationen (Orthofotos) gewerblich verwertet werden (so etwa Art. 19 GeoIG; § 13 GeoIG-ZG vom 29. März 2012, BGS 215.71). – Zur föderalistischen Ordnung des Datenschutzes s. oben Rz 1.13 ff.

151 JÖHRI, Art. 17 DSG N 1; BSK DSG-BALLENEGGER, Art. 17 N 1. Zur Frage der Rechtsetzungsstufe siehe JÖHRI, Art. 17 DSG N 18 ff.; BSK DSG-BALLENEGGER, Art. 17 N 25.

152 Siehe dazu Rz 15.136 ff.

fachbezogener Geobasisdaten eine systematische Tätigkeit i.S.v. Art. 18 DSG darstellt, kann offen bleiben. Das Geoinformationsgesetz stellt auf jeden Fall die erforderliche Gesetzesgrundlage dar, die eine Informationspflicht der betroffenen Personen erübrigt (Art. 18a Abs. 3 und Abs. 4 lit. a DSG).

15.105 Auch bei datenschutzrelevanten Geobasisdaten gilt der Grundsatz, dass jedes Bekanntgeben von Personendaten eine Verletzung der Persönlichkeit ist und die Handlung nur rechtmässig ist, wenn bestimmte Voraussetzungen erfüllt sind. Art. 19 Abs. 1 DSG verweist zunächst auf allenfalls bestehende gesetzliche Regelungen (Sonderregeln), nennt dann zusätzlich vier Fälle, die das Bekanntgeben rechtfertigen: a. wenn der Empfänger die Angaben für die Erfüllung seiner gesetzlichen Aufgaben unbedingt braucht, b. wenn die betroffene Person im Einzelfall einwilligt, c. wenn die betroffene Person ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt hat oder d. wenn der Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert, um ihn an der Durchsetzung von Rechtsansprüchen zu hindern. Für Geobasisdaten bestehen *in den Fachgesetzen* (etwa RPG, USG mit der Umsetzung der Aarhus-Konvention) insbesondere aber *im Geoinformationsgesetz die rechtlichen Grundlagen* für die Bekanntgabe und Weitergabe von Informationen. Weitere Rechtfertigungsgründe sind nicht erforderlich. Immerhin könnte bei einer Lücke im fachrechtlichen Bereich der Rechtfertigungsgrund nach Buchstabe a „Bedarf für die Erfüllung einer gesetzlichen Aufgabe“ zur Anwendung kommen.

15.106 Art. 19 Abs. 2 DSG erlaubt es den Bundesorganen ausdrücklich auf Anfrage Namen, Vornamen, Adresse und Geburtsdatum bekanntzugeben. Diese *Angaben sind zugänglich, weil sie ohnehin mehr oder weniger bekannt* und bei Anfragen auf der kommunalen Einwohnerkontrolle sowieso erhältlich sind[153]. Die Öffentlichkeit der Geobasisdaten zum Grundbuch (Art. 970 Abs. 2 ZGB) entspricht dieser Grundsatzregelung[154].

15.107 Das Datenschutzgesetz regelt auch den Zugang im Abrufverfahren (Art, 19 Abs. 3 DSG) und mittels automatisierter Informations- und Kommunikationsdienste (Art. 19 Abs. 3bis DSG). Diese Regelung deckt sich weitgehend mit den Anliegen und der Zielsetzung der Geodatenbewirtschaftung.

15.108 Die Gesetzesgrundlage für Datenbekanntgaben nach Art. 19 DSG ist nicht nötig, wenn die *Personendaten für Forschungs-, Planungs- und Statistikzwecke* weitergegeben werden (Art. 22 DSG)[155]. In diesem Fall müssen die Daten jedoch anonymisiert werden (sobald es der Zweck des Bearbeitens erlaubt), der Empfänger darf die Daten ohne Zustimmung der

153 JÖHRI, Art. 19 DSG N 67.
154 Siehe dazu Rz 15.125 ff.
155 JÖHRI, Art. 19 DSG N 8.

Bundesorgane nicht weitergeben und die Ergebnisse müssen so veröffentlicht werden, dass die betroffenen Personen nicht bestimmt werden können. Mit dieser Regelung können Bundesbehörden Grundlagen für Planungen umfassend erstellen und in die Planungsarbeit einfliessen lassen, auch wenn eine Regelung im Fachgesetz (noch) fehlt oder Personeninformationen enthalten sind[156].

cc) Bearbeiten durch kantonale und kommunale Verwaltungseinheiten

15.109 Für das Bearbeiten datenschutzrelevanter Geobasisdaten des kantonalen und kommunalen Rechts haben die *Kantone eigenständige Regelungen* zu treffen und diese mit dem bestehenden kantonalen Datenschutzgesetz zu koordinieren.

15.110 Im Recht der raumwirksamen Tätigkeiten erfüllen die Kantone im Rahmen der *Organisationsautonomie* selbständige Aufgaben. So entscheiden sie nach eigenen Bedürfnissen, ob und in welcher Form Geobasisdaten des kantonalen oder kommunalen Rechts erfasst werden, und sie bestimmen, wer die Geobasisdaten bewirtschaftet.

15.111 Die bundesstaatlichen *Zuständigkeiten* des Rechts der raumwirksamen Tätigkeiten *decken sich* mit jenen im Datenschutz *nicht*: Das eidgenössische Datenschutzgesetz gilt für die gesamten Tätigkeiten der Bundesverwaltung (und der Privaten); kantonales Datenschutzrecht dagegen bestimmt die Rahmenbedingungen für das Handeln der kantonalen und kommunalen Behörden. Im Recht der raumwirksamen Tätigkeiten vollziehen kantonale Verwaltungseinheiten direkt oder aufgrund von Ausführungsbestimmungen Bundesrecht; sie bearbeiten regelmässig Geobasisdaten des Bundesrechts. Für diese Tätigkeit sieht das eidgenössische Geoinformationsrecht im Sinne einer Harmonisierung eine Sonderregelung vor: *Beim Bearbeiten von Geobasisdaten des Bundes kommt auf jeden Fall Bundesdatenschutzrecht zur Anwendung*[157]. Dies ergibt sich aus den gesetzlichen Verweisen – nach Art. 11 GeoIG sind Art. 16–25 DSG auf Geobasisdaten des Bundesrechts anzuwenden – und wird in der Botschaft zum Geoinformationsgesetz bestätigt: „Das Gesetz legt fest, dass auf alle Geobasisdaten des Bundesrechts […] die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG) Anwendung finden. Damit wird erreicht, dass für alle Geobasisdaten des Bundesrechts eine einheitliche Regelung des Datenschutzes gilt, nämlich die des Bundes, und zwar unabhängig davon, ob eine Behörde des Bundes, des

156 Oft erfordert die Erarbeitung eines Projekts Vorabklärungen, aus denen ein Regelungsbedarf erst erkennbar wird. Die Vorschläge können dann mit Fachgrundlagen untermauert werden.

157 HUSER, Grundzüge, 155 m.w.H.

Kantons oder der Gemeinde oder eine im (hoheitlichen) öffentlichen Auftrag handelnde Privatperson die *personenrelevanten Geobasisdaten* bearbeitet“[158].

15.112 Kantonales Datenschutzrecht kommt somit dann nicht zur Anwendung[159], wenn kantonale Verwaltungseinheiten Geobasisdaten des Bundesrechts bearbeiten[160]. Grundsätzlich muss ein kantonales Amt für Umwelt bei der Bearbeitung datenschutzrelevanter Geobasisdaten des Umweltrechts das eidgenössische Datenschutzgesetz zur Hand nehmen und sich für das Bewirtschaften kantonaler oder kommunaler Geobasisdaten an das kantonale Recht halten. Das führt zu *Unsicherheiten*[161], zumal sich kantonale oder kommunale Geobasisdaten im Normalfall auf die Georeferenzdaten der amtlichen Vermessung stützen, die ja Geobasisdaten des Bundesrechts sind[162]. Die kantonalen Geoinformationsgesetze orientieren sich regelmässig an der im Datenschutzrecht üblichen Kompetenzaufteilung und erklären – ohne Differenzierung[163] – die kantonalen Regeln für anwendbar[164]. Nachdem die kantonalen Datenschutzgesetze sich inhaltlich mit den Mindestanforderungen des eidgenössischen Datenschutzrechts und den verfassungsmässigen Grundrechten decken, besteht eine materielle Koordination des Datenschutzes.

3. Bearbeiten nach dem Geoinformationsrecht

a) Einleitung

15.113 *Geobasisdaten* des Bundesrechts *ohne Datenschutzrelevanz* können Persönlichkeitsrechte auf jeden Fall nicht verletzen. Sie sind kein Thema des Datenschutzes. Zu regeln ist lediglich der Umgang mit den bewirtschafteten Daten im öffentlichen Interesse. Diese Funktion übernimmt das Geoinformationsrecht.

---

158 Botschaft GeoIG, 7851 (Hervorhebungen durch den Autor). Siehe auch KETTIGER, URP, 775.

159 Anders das Öffentlichkeitsgesetz des Bundes: Dieses Gesetz gilt für die Kantone nicht (vgl. Botschaft BGÖ, 1977). Es gilt auch dann nicht, wenn die Kantone Bundesrecht umsetzen (BRUNNER/MADER, Einleitung Rz 66; **a.M.** KETTIGER, URP, 775).

160 KETTIGER, Geheimhaltung und Öffentlichkeit, 54 f. RUDIN (4 f.) spricht dem Geoinformationsgesetz die (datenschutzrechtliche) Verfassungsmässigkeit ab, soweit es in die kantonale Hoheit eingreift.

161 Siehe dazu auch oben Rz 8.36 ff.

162 Der Bund hätte mit Art. 75a Abs. 3 BV die Kompetenzen, den Datenschutz von Geobasisdaten auf allen Ebenen gesamtschweizerisch zu harmonisieren; diese Kompetenz übt er aber nur für die Geobasisdaten des Bundesrechts aus (s. dazu HUSER, Vermessungsrecht, Rz 667; DERS., Grundzüge, 156; RUDIN, 3, spricht dem Bund die Kompetenz ab, materielles Datenschutzrecht zu setzen, das über seine Organe hinaus wirke).

163 Immerhin lässt das Gesetz über Geoinformation des Kantons Luzern (vom 3. September 2003, SRL Nr. 39) die Anwendung beider Gesetzgebungen zu, indem es in Art. 7 und 8 auf die Vorschriften des Bundes und des Kantons über den Datenschutz verweist.

164 Etwa § 9 Abs. 2 Gesetz vom 29. März 2012 über Geoinformation im Kanton Zug (Geoinformationsgesetz, GeoIG-ZG; BGS 215.71), § 4 Gesetz vom 24. Mai 2011 über die Geoinformation im Kanton Aargau (Kantonales Geoinformationsgesetz, KGeoIG; AGS 740.100), ebenso § 8 ff. Kantonales Geoinformationsgesetz [des Kantons Zürich] vom 24. Oktober 2011 (KGeoIG; LS 704.1), § 5 Gesetz [des Kantons Thurgau] vom 29. Juni 2011 über Geoinformation (RB 211.441), Art. 7 Geodatenverordnung [des Kantons Bern] vom 27. April 2005 (GeoIV; BSG 215.341.2); BELSER/NOUREDDINE, § 8 N 34.

Das Geoinformationsgesetz wirkt in seiner Querschnittfunktion[165] auf die Fachgesetze des Rechts der raumwirksamen Tätigkeiten ein. Es enthält namentlich *Bestimmungen über die Öffentlichkeit der Geobasisdaten* des Bundesrechts sowie die Rahmenbedingungen und Verfahrensgrundsätze über den Zugang und die Veröffentlichung (Zugangsberechtigungsstufen, Vorgehen zur Bewilligung des Zugangs und Ort der Datenabgabe). **15.114**

Diese Regelungen sind für *Geobasisdaten des Bundesrechts abschliessend*, soweit nicht ein Spezialgesetz über raumwirksame Tätigkeiten (des Bundes) Abweichungen vorsieht (Art. 2 Abs. 2 GeoIG)[166]. **15.115**

Die *Kantone* haben für ihre und die kommunalen Geobasisdaten, die keine Datenschutzrelevanz haben, *analoge Regelungen* getroffen. **15.116**

b) Zugangsberechtigungsstufen

Der Zugang zu den Geobasisdaten des Bundesrechts wird im Sinne einer Interessenwahrung[167] nach *drei Zugangsberechtigungsstufen* ermöglicht (Art. 21 GeoIV): **15.117**

- Die öffentlich zugänglichen Geobasisdaten (Stufe A): Diese Geobasisdaten können ohne Bewilligung frei eingesehen werden. Falls die Einsicht im Einzelfall infolge des Berufs- oder Amtsgeheimnisses oder wegen anderen Grundrechten beschränkt werden soll, ist eine Abweisungsverfügung zu erlassen.
- Die beschränkt öffentlich zugänglichen Geobasisdaten (Stufe B): Wer Einsicht nehmen will, muss sein (besonderes) Interesse nachweisen (GeoIG) oder glaubhaft machen (ZGB).
- Die nicht öffentlich zugänglichen Geobasisdaten (Kategorie C): Die Einsicht ist den Behörden und Personen vorbehalten, die mit den Informationen arbeiten müssen. Dritten werden sie nicht offengelegt.

Die *Geoinformationsverordnung teilt* jedem Geobasisdatum die *Zugangsberechtigungsstufe zu*. Die Interessenabwägung nach Art. 10 GeoIG hat der Bundesrat[168] an sich mit der Zuteilung der Zugangsberechtigungsstufe der einzelnen Geobasisdaten im Datenkatalog (Anhang zur Geoinformationsverordnung) verabschiedet. Der Zugang zum jeweiligen Geodatensatz wird jedoch im Einzelfall noch definitiv zu beurteilen sein, wie dies in der Geoinformationsverordnung auch für die Geobasisdaten der Zugangsberechtigungsstufe A vorgesehen ist (Art. 22 GeoIV). **15.118**

---

165 HUSER, Grundzüge, 147 f.
166 HUSER, Grundzüge, 146 f.
167 Siehe dazu HUSER, Grundzüge, 153 f.
168 Das Gesetz erklärt in Art. 12 GeoIG die für das Erheben, Nachführen und Verwalten der Geobasisdaten zuständige Stelle für zuständig; so wohl auch KETTIGER, Geheimhaltung und Öffentlichkeit, 54.

c) Zugangsgewährung

15.119 Die für das Erheben, Nachführen und Verwalten der Geobasisdaten zuständige Stelle kann den Zugang zu Geobasisdaten des Bundesrechts sowie deren *Nutzung und Weitergabe von einer Einwilligung abhängig machen* (Art. 12 Abs. 1 GeoIG). Die Einwilligung erfolgt mit Verfügung, Vertrag oder durch organisatorische und technische Zugangskontrollen (Art. 12 GeoIG).

15.120 Die *Verfügungsform* ist in jedem Fall *zwingend*, wenn der Zugang verweigert werden soll (Art. 26 GeoIV). Die vertragliche Regelung soll den Verwaltungsbehörden die Möglichkeit eröffnen, "mit kommerziellen Nutzerinnen und Nutzern jeweils auf die spezifische Bedürfnisse angepasste Regelungen […]"[169] zu treffen. Grossbezüger sollen vertraglich gebunden werden können.

15.121 Die Gewährung des *Zugangs durch organisatorische oder technische Zugangskontrollen* deckt die Bedürfnisse der Online-Nutzung ab und ermöglicht eine effiziente Bewirtschaftung der Datenbasis. Wird der Vertragsabschluss oder die Einwilligung mittels organisatorischer oder technischer Zugangskontrollen verweigert, so kann die betroffene Person eine anfechtbare Verfügung verlangen (Art. 26 Abs. 2 GeoIV).

d) Zugangsort

15.122 Grundsätzlich hat das kantonale Recht diese Organisationsfrage zu klären. In der Regel werden die Geobasisdaten von einer speziell bezeichneten *zentralen*[170] *Fachstelle*, wie etwa GIS-Abteilung oder Vermessungsamt zur Verfügung gestellt und zur Nutzung bereitgehalten. Es kann auch das jeweilige Fachamt (Amt für Raumplanung, Amt für Umweltschutz, Landwirtschaftsamt usw.) mit der Abgabe der Fachdaten betraut sein, was mit Blick auf die Beratung des Antragsstellers oder Anfragers Sinn macht.

4. Bearbeiten nach Grundbuchrecht im Speziellen

a) Einleitung

15.123 Angaben über dingliche *Rechte an Grund und Boden* (Eigentum, Dienstbarkeiten) *verknüpfen geografische Sachverhalte mit Personenangaben.* Das Grundbuch fixiert (zusammen mit der amtlichen Vermessung) Grundstücksflächen und ordnet diese berechtigten Personen zu. Grundbuchangaben sind somit Geobasisdaten des Bundesrechts mit Datenschutzrelevanz.

169 Botschaft GeoIG, 7852 f.
170 So verlangt es bspw. Art. 17 Abs. 3 ÖREB-Katasterverordnung (SR 510.622.2).

Damit das Grundeigentum geachtet werden kann, müssen die Rechte und die Berechtigten[171] auch publiziert werden.

Das Datenschutzgesetz des Bundes kommt bei öffentlichen Registern des privaten Rechts nicht zur Anwendung (Art. 2 Abs. 2 lit. d DSG), weil die Bearbeitung dieser Daten nach eigenen, sehr detaillierten und formellen Vorschriften abläuft[172]. Solche Vorschriften finden sich für die Grundbuchdaten im *Schweizerischen Zivilgesetzbuch*, in Bezug auf die Einrichtung und Rechtswirkung des elektronischen Grundbuchs (Art. 942 Abs. 3 und Art. 949a ZGB) und die Auskunft und Veröffentlichung der Grundbuchangaben (Art. 970 und 970a ZGB). Diese Regeln werden ergänzt durch die Einzelheiten in der Grundbuchverordnung (Art. 26–34 GBV) und – soweit nötig - in der Geoinformationsverordnung. **15.124**

b) Zugang mit oder ohne Interesse

Das ZGB unterscheidet zwischen den Grundbuchdaten, die ohne *ein Interesse glaubhaft* zu *machen*, eingesehen werden können, und den Grundbuchdaten, bei denen ein Interesse glaubhaft gemacht werden muss. **15.125**

Der grösste Teil der rechtswirksamen *Grundbuchdaten* ist *öffentlich* und kann ohne Glaubhaftmachen eines besonderen Interesses eingesehen und abgegeben werden (Art. 970 Abs. 2 ZGB): Bezeichnung der Grundstücke und Grundstücksbeschreibungen, Namen und Identifikation des Eigentümers, die Eigentumsform und das Erwerbsdatum. Der Bundesrat hat gestützt auf Art. 970 Abs. 3 ZGB auch die Dienstbarkeiten und Grundlasten sowie einen Grossteil der Anmerkungen als allgemeinzugänglich erklärt (Art. 26 GBV). Diese Offenheit ist sachgerecht, drücken doch die Einträge im Grundbuch dingliche Rechtspositionen aus, die gegenüber jedermann wirken. Soll sich die Allgemeinheit an die Schranken halten, die sich aus dem Eigentum und dessen Nutzung ergeben, muss sie die Schranken kennen, also auch erfahren können, wer welche Rechte an Grundstücken in welchem Umfang besitzt. **15.126**

Alle weiteren Angaben des Grundbuchs, wie etwa die historischen Angaben oder die Rechtsgrundausweise (Verträge mit allfälligen Kaufpreisen), sind nicht allgemein einsehbar. Wer Einsicht nehmen will, muss ein *Interesse glaubhaft machen* (Art. 970 Abs. 1 ZGB). **15.127**

Für verschiedene Berufsgruppen ist dieses Einsichtsinteresse gesetzlich anerkannt, soweit sie die Informationen zur Erfüllung ihrer Aufgabe benötigen (Art. 28 GBV): Urkundspersonen, im Geometerregister eingetragene Ingenieur-Geometerinnen und Ingenieur-Geometer, Banken, die Schweizerische Post, Pensionskassen, Versicherungen und vom Bund anerkannte **15.128**

171 Name, Vorname, Geburtsdatum, Heimatort – ähnlich wie bei Art. 19 Abs. 2 DSG.
172 BELSER/NOUREDDINE, § 7 N 65; WALDMANN/BICKEL, § 12 N 38; HUSER, Geo-Informationsrecht, 175.

Institutionen aus dem bäuerlichen Bodenrecht sowie die im Anwaltsregister eingetragenen Rechtsanwältinnen und Rechtsanwälte.

c) Zugangsort

15.129 Informationen und Auskünfte können *auf dem Grundbuchamt*, d.h. mündlich vor Ort oder per Telefon erfragt werden.

15.130 Die Kantone können die allgemein zugänglichen Grundbuchdaten des Hauptbuches zudem *im Internet* zugänglich machen (Art. 27 Abs. 1 GBV). Vorausgesetzt ist ein Entscheid des kantonal zuständigen Organs. Ein Beschluss durch die kantonale Exekutive in einer Verordnung genügt, nachdem die materiell wichtigen Schranken in der Bundesgesetzgebung umfassend vorgegeben sind und kein gesetzgeberischer Handlungsspielraum besteht.

15.131 *Auskünfte* können nur *für ein bestimmtes Grundstück* erteilt werden. Fragen über Eigentümer oder dinglich berechtigte Personen werden nicht beantwortet. Diese Einschränkung gilt für Auskünfte auf dem Grundbuchamt, per Telefon oder im Internet (Art. 26 Abs. 2 GBV).

15.132 Bei der elektronischen Auskunft aus dem Internet muss die technische Installation sicherstellen, dass *keine Serienabfragen* möglich sind (Art. 27 Abs. 2 GBV). In der Praxis handhaben die Kantone diese Schranke sehr unterschiedlich. Verschiedene Kantone haben das EDV-System so eingerichtet, dass im Suchfeld Ortsangaben oder Grundstücknummern eingegeben werden können. Andere Kantone teilen einem Anfragenden eine bestimmte Anzahl Passwörter zu, mit denen je eine Abfrage möglich ist. Oft wird die Serienabfrage unterbunden, indem pro Tag nur eine bestimmte Anzahl Grundstücke besucht werden kann. Es lohnt sich, die jeweilige Praxis beim Kanton nachzufragen.

V. Rechtsschutz

15.133 Für die vorliegende Darstellung wird der Begriff Rechtsschutz weit verstanden und umfasst alles, womit sich eine Person, die in ihren Persönlichkeits- bzw. Grundrechten verletzt ist oder sich verletzt glaubt, gegen eine Veröffentlichung von Geodaten und Geobasisdaten wehren kann. Dazu gehört das Auskunftsrecht (unten Rz 15.134 f.), das Sperrrecht (unten Rz 15.136 ff.) und das Klage- bzw. Beschwerderecht (unten Rz 15.147 ff. und Rz 15.153 ff.).

1. Auskunftsrecht

15.134 Wer als Privatunternehmung Geländeaufnahmen mit datenschutzrelevanten Inhalten erhebt und in einem Informationssystem verwaltet, will diese Aufnahmen wirtschaftlich verwerten. Er hat ein Interesse daran, die Aufnahmen öffentlich bekanntzumachen. Der

Privatunternehmer ist als *Inhaber datenschutzrelevanter Informationssysteme* zur Auskunft verpflichtet. Der Anspruch richtet sich nach Art. 8–10 DSG. Es kommen die allgemeinen Grundsätze zur Anwendung.

Im Geoinformationsgesetz ist die Bekanntgabe von *Geobasisdaten*, die im Rahmen der Verwaltungstätigkeit bei Behörden anfallen, *eine Hauptaufgabe* (Art. 1 GeoIG). Eine Pflicht zur Bekanntgabe der vorhandenen Datensammlungen ergibt sich für die Bundesbehörden auch aus dem Bundesgesetz über die Öffentlichkeit. Bei kantonalen Behörden ist zunächst zu prüfen, ob ein Öffentlichkeitsprinzip für die Verwaltungstätigkeit eingeführt ist, das bei kantonal und kommunal geregelten Geobasisdaten zur Anwendung kommt. Alsdann kann sich der Private ebenfalls auf Art. 11 GeoIG berufen, soweit er Auskunft über Datensammlungen erhalten will, die der Kanton beim Vollzug des Bundesrechts (v.a. im Umweltbereich) führt. Zudem muss im kantonalen Recht (GeoIG oder in einem Fachgesetz) geprüft werden, ob und wie weit für kantonal und kommunal geregelte Geobasisdaten ein Zugangsanspruch besteht. **15.135**

2. Sperrrecht

Das Sperrrecht ist für die verschiedenen Arten von Geoinformationen *unterschiedlich geregelt*. **15.136**

a) Sperre von Geodaten

Die Sperre datenschutzrelevanter Geodaten betrifft die *privaten Nutzerinnen und Nutzer*; sie *richtet sich nach dem eidgenössischen Datenschutzgesetz*. Danach kann eine Person, die in ihrer Persönlichkeit verletzt ist, verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekanntgegeben oder die Personendaten berichtigt oder vernichtet werden (Art. 15 Abs. 1 DSG). **15.137**

Die Sperrung ist im Rahmen einer *Klage nach Art. 28a ZGB* zu verlangen (Art. 15 DSG). **15.138**

b) Sperre von Geobasisdaten des Bundesrechts

Für Datensammlungen der Bundesbehörden besteht ein *allgemeines, datenschutzrechtliches Sperrrecht* (Art. 20 DSG). Danach kann eine betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, vom verantwortlichen Bundesorgan verlangen, dass es die Bekanntgabe von bestimmten Personendaten[173] sperrt. Sie muss die Daten, die gesperrt werden sollen, konkret bezeichnen. Das Bundesorgan verweigert die Sperrung oder hebt sie **15.139**

173 Botschaft DSG 1988, 472; JÖHRI, Art. 20 DSG N 14.

auf, wenn eine Rechtspflicht zur Publikation besteht oder die Erfüllung seiner Aufgaben sonst gefährdet wäre.

15.140 Für *Geobasisdaten des Bundesrechts gilt das Sperrrecht* ebenfalls (Art. 11 GeoIG i.V.m. Art. 20 DSG), sofern datenschutzrelevante Geobasisdaten zur Diskussion stehen. Für Geobasisdaten ohne Datenschutzrelevanz kann der Zugang einzig zum Schutz des öffentlichen Interesses im Einzelfall verwehrt werden (Art. 22 Abs. 2 lit. a–g GeoIV). Auch der Private kann eine Sperrung nicht wegen der Verletzung seiner Persönlichkeitsrechte anrufen, soweit das Datenschutzgesetz nicht zur Anwendung kommt.

15.141 Die *Veröffentlichung von datenschutzrelevanten Daten im Internet bedarf einer materiell gesetzlichen Grundlage* (Art. 19 Abs. 3 DSG). Diese Grundlage ist in der Geoinformationsverordnung für alle Geobasisdaten vorhanden. Ohne Rücksicht darauf, ob die Geobasisdaten des Bundesrechts datenschutzrelevant sind oder nicht, müssen sie im Internet durch Darstellungsdienste und durch Download-Dienste angeboten und zugänglich gemacht werden (Art. 43 GeoIV). Sperrmöglichkeiten sind nicht vorgesehen.

c) Sperre von Geobasisdaten des kantonalen und kommunalen Rechts

15.142 Das *kantonale Recht entscheidet*, ob und unter welchen Voraussetzungen Geobasisdaten, die ihren Rechtsbezug im kantonalen oder kommunalen Recht haben, gesperrt werden können. Im Einzelfall ist somit die Gesetzgebung des Kantons zu konsultieren.

15.143 Es darf grundsätzlich davon ausgegangen werden, dass die *kantonalen Bestimmungen sich am Bundesrecht* und den kantonalen Datenschutzgesetzen *orientieren*.

d) Sperre von Geobasisdaten des Grundbuchs im Besonderen

Eine Sperre von Grundbuchdaten auf Antrag eines Grundeigentümers oder dinglich Berechtigten *sehen das Zivilgesetzbuch* (Art. 970 ZGB) und die Grundbuchverordnung (Art. 26 GBV) *nicht vor*. Die Einsichtnahme auf dem Grundbuchamt ist jederzeit möglich und kann – auch im Einzelfall – nicht abgelehnt werden. **15.144**

Die *Kantone entscheiden selbstständig* über eine Publikation im Internet (Art. 27 Abs. 1 GBV)[174]. Ihre Gesetzgebungskompetenzen können sie ganz, teilweise oder gar nicht nutzen. Das kantonale Recht kann eine Sperrung der Publikation der Grundbuchdaten im Internet auf Antrag eines betroffenen Grundeigentümers oder eines dinglich Berechtigten vorsehen. Diese Lösung ist mit Art. 19 Abs. 3bis DSG koordiniert. Der Kanton muss aber die Publikation in öffentlich zugänglichen Datennetzen in einem Rechtssatz beschliessen, wobei ein Gesetz im materiellen Sinn genügt[175]. Solange keine Regelung vorliegt, ist die Veröffentlichung im Internet nicht zulässig. **15.145**

Je nach kantonaler Regelung führt dieses Zugangs- bzw. Sperrsystem zu *inkonsequenten Resultaten* und wird von den technischen Möglichkeiten gleichsam ad absurdum geführt. In der Tat können – sofern die Publikation im Internet kantonal vorgesehen ist – Angaben per Smartphone über den Grundstückeigentümer im Internet abgefragt werden. Trifft der Suchende auf gesperrte Stellen, kann er mit dem gleichen Gerät beim Grundbuchamt nachfragen. Dort erhält er die Information sofort oder zumindest ohne Verzögerung. **15.146**

3. Rechtsschutz bei Verletzung der Persönlichkeitsrechte durch Private

Bei der *Verletzung der Persönlichkeitsrechte durch Private* stehen nur Geodaten zur Diskussion[176]. Geobasisdaten hingegen sind im Rahmen der Persönlichkeitsverletzung durch Verwaltungseinheiten des Bundes, des Kantons oder der Gemeinden zu behandeln. **15.147**

a) Klage nach Art. 28a ZGB

Zum Schutz vor persönlichkeitsverletzenden Darstellungen kann der Private verlangen, dass die Datenbearbeitung beendet oder die Bekanntgabe an Dritte gesperrt wird oder die Personenangaben berichtigt oder vernichtet werden. Er kann sich dabei auf eine *Verletzung des ZGB und des DSG* berufen. Eine Sperrung ist beim Zivilrichter mit der Klage nach **15.148**

---

174 Siehe dazu oben Rz 15.129 ff.

175 Diese Rechtsform wird auch beim Abrufverfahren für Personendaten nach Art. 19 Abs. 1 DSG befürwortet, soweit es nicht um besonders schützenswerte Daten oder Persönlichkeitsprofile geht (WALDMANN/BICKEL, § 12 N 96).

176 Siehe dazu Rz 15.60 ff.

Art. 28a ZGB zu beantragen. Der Private kann sich bei Klagen gegenüber einem anderen Privaten auf Grundrechte nur berufen, wenn diesen Drittwirkung zukommt.

15.149 Die *Klage* steht unabhängig davon offen, welcher Private für die Datensammlung verantwortlich ist; sie kann sich insbesondere *auch gegen den faktischen Inhaber* der Sammlung richten[177].

15.150 Über die Klagen zur Durchsetzung des Auskunftsrechts gegen Private entscheidet der Richter in einem *einfachen und raschen Verfahren* (Art. 15 Abs. 4 DSG[178]).

b) Meldung an EDÖB

15.151 Die Durchsetzung der Ansprüche nach Art. 15 DSG kann für die klagende Partei mit einem *Kosten- und Prozessrisiko* verbunden sein[179]. Der Private kann die Verletzung der Datenschutzregeln deshalb in jedem Fall und unabhängig von der Geltendmachung zivilrechtlicher Ansprüche[180] dem eidgenössischen Öffentlichkeits- und Datenschutzbeauftragten (EDÖB, Beauftragter) unterbreiten (Art. 29 DSG).

15.152 Der Beauftragte kann im Privatrechtsbereich *Abklärungen vornehmen und Empfehlungen abgeben,* wenn a. Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler), b. Datensammlungen registriert werden müssen oder c. eine Informationspflicht besteht. Wird eine Empfehlung nicht befolgt oder abgelehnt – wie dies beim Street-View-Entscheid der Fall war –, so kann der Beauftragte die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen (Art. 29 DSG)[181]. Im Verfahren nach Art. 29 DSG hat die Privatperson, welche die Untersuchung ausgelöst hat, keine Parteirechte[182].

177 ROSENTHAL, Art. 3 lit. i DSG N 109.
178 ROSENTHAL, Art. 15 DSG N 2.
179 ROSENTHAL, Art. 15 DSG N 2; s.a. oben Rz 1.46 f.
180 ROSENTHAL, Art. 15 DSG N 3.
181 Dazu JÖHRI, Art. 33 DSG N 5.
182 ROSENTHAL, Art. 29 DSG N 8.

4. Rechtsschutz bei Verletzung der Persönlichkeitsrechte durch Organe der öffentlichen Hand

a) Im Allgemeinen

Die *Verwaltungseinheiten* – im Datenschutzgesetz Organe der öffentlichen Hand genannt – bearbeiten im Rahmen der öffentlich-rechtlichen Aufgaben ausschliesslich Geobasisdaten (Legalitätsprinzip[183]). Der Rechtsschutz richtet sich nach Bestimmungen des Verwaltungsrechts. **15.153**

Die Durchsetzung datenschutzrechtlicher Ansprüche im öffentlich-rechtlichen Bereich kann durch *Erlass einer Feststellungsverfügung* eingeleitet werden[184]. Dabei kann die Beseitigung oder Korrektur bestehender Datensammlungen oder einzelner Einträge verlangt werden. Der Gesuchsteller muss selbstverständlich sein Interesse an der beantragten Handlung darlegen (so etwa Art. 25a VwVG). **15.154**

b) Beim Bearbeiten von Geobasisdaten

Der Rechtsschutz ist von jener *Behörde* zu gewährleisten*, die für die Datenbearbeitung verantwortlich ist.* Dies gilt nicht nur, wenn Datenschutzverletzungen beanstandet werden, sondern auch, wenn der Zugang zu den Geobasisdaten des Bundesrechts verweigert wird[185]. **15.155**

Für Geobasisdaten des Bundesrechts, die von Bundesorganen bearbeitet werden, ergeben sich *datenschutzrechtliche Abwehrrechte aus Art. 25 DSG* (i.V.m. Art. 11 GeoIG). Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, widerrechtliches Bearbeiten zu unterlassen, die Folgen eines widerrechtlichen Bearbeitens zu beseitigen oder die Widerrechtlichkeit der Tätigkeit festzustellen. Es besteht ein Anspruch auf eine Verfügung[186]. Gegen diese Verfügungen kann nach den allgemeinen Bestimmungen über die Bundesrechtspflege Beschwerde beim Bundesverwaltungsgericht erhoben werden[187]. Es kommt das VwVG zur Anwendung. **15.156**

Werden Geobasisdaten des Bundesrechts von kantonalen Organen bearbeitet, kommt *kantonales Verwaltungsverfahrensrecht*[188] zur Anwendung. Die Klagemöglichkeiten nach dem eidgenössischen Datenschutzgesetz kommen nicht zum Zug, da die kantonalen Behörden **15.157**

183 Siehe dazu Rz 15.101 ff.
184 Siehe oben Rz 7.72 ff.
185 Siehe dazu Rz 15.119 ff.
186 JÖHRI, Art. 25 DSG N 37.
187 JÖHRI, Art. 25 DSG N 39 und Art. 33 DSG N 2.
188 JÖHRI, Art. 33 DSG N 7.

keine Bundesorgane sind, selbst wenn sie Bundesrecht vollziehen. Gegen letztinstanzliche, kantonale Entscheide ist die Beschwerde in öffentlich-rechtlichen Angelegenheiten ans Bundesgericht zu erheben[189].

15.158 *Für Geobasisdaten des kantonalen oder kommunalen Rechts gilt das kantonale Recht*. Dieses kann – analog zum Bundesrecht im Geoinformationsgesetz - speziell auf die Nutzungsbedürfnisse abgestimmte Spezialregeln enthalten und einzelne Bestimmungen des kantonalen Datenschutzgesetzes ergänzend zur Anwendung bringen. Die bestehenden Gesetze verweisen regelmässig auf das kantonale Datenschutzrecht[190]. Die kantonale Verwaltungsverfahrensgesetzgebung wird den Verfahrensablauf und die innerkantonalen Beschwerdemöglichkeiten bestimmen. Gegen letztinstanzliche, kantonale Entscheide ist die Beschwerde in öffentlich-rechtlichen Angelegenheiten ans Bundesgericht zulässig (Art. 82 ff. BGG)[191].

c) Überwachung durch Datenschutzbeauftragten

15.159 Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte überwacht die Einhaltung des eidgenössischen Datenschutzgesetzes und der übrigen Datenschutzvorschriften des Bundes *durch die Bundesorgane*[192]. Er kann dieser Überwachung aus eigenem Antrieb oder aufgrund von Meldungen Dritter Nachforschungen machen, den Sachverhält näher abklären oder den verantwortlichen Bundesorganen Empfehlungen abgeben. Schliesslich kann der Beauftragte eine Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen, wenn seine Empfehlung nicht befolgt wird (Art. 27 Abs. 2–5 DSG)[193].

15.160 Wie weit *kantonale Datenschutzbeauftragte* das Bearbeiten der Geobasisdaten durch kantonale oder kommunale Verwaltungseinheiten überwachen können, ist den kantonalen Regelungen zu entnehmen. Der EDÖB jedenfalls ist nicht zuständig und zwar auch dann nicht, wenn Geobasisdaten des Bundes durch kantonale Einheiten bearbeitet werden. Verweist das kantonale Geoinformationsrecht auf die Datenschutzregelung, ist die Kontrolle und Interventionsmöglichkeit des (kantonalen) Datenschutzbeauftragten aber regelmässig mitenthalten.

---

189 Für diesen Rechtsweg s. die überzeugende Begründung bei JÖHRI, Art. 33 DSG N 7.
190 So etwa § 8 ff. KGeoIG-ZH, § 5 Gesetz über Geoinformation (Kanton Thurgau); § 9 GeoIG-ZG.
191 JÖHRI (Art. 33 DSG N 5) schlägt diese Beschwerdeart sogar vor, wenn in der Sache selber das eidgenössische Datenschutzgesetz als Bundeszivilrecht zur Anwendung gelangt.
192 Verwalten und bearbeiten kantonale Verwaltungsstellen Geobasisdaten des Bundesrechts, kommt die Aufsicht des EDÖB nicht zum Tragen.
193 JÖHRI, Art. 27 DSG N 1; s.a. oben Rz 7.75.

VI. Checkliste

1. Enthalten die Geodaten Informationen über genau bestimmte oder bestimmbare Personen?

– *Ja:* weiter bei Frage 2
– *Nein:* keine Datenschutzrelevanz

2. Werden die Informationen durch eine Privatperson bearbeitet?

– *Ja:* weiter bei Frage 3
– *Nein:* weiter bei Frage 7

3. Verletzt das Bearbeiten von Geodaten die Persönlichkeit einer konkreten Person?

– *Ja:* weiter zur Frage 4
– *Nein:* keine Konsequenzen

4. Bestehen Rechtfertigungsgründe für die Persönlichkeitsverletzung?

– *Ja:* keine weiteren Konsequenzen
– *Nein:* weiter zur Frage 5

5. Kann die Verletzung vollständig rückgängig gemacht werden?

– *Ja:* datenschutzrechtlichen Massnahmen umsetzen; weiter zur Frage 6
– *Nein:* weiter zur Frage 9

6. Kann die verletzte Person die Umsetzung durchsetzen?

– *Ja:* Umsetzung bzw. Berichtigung verlangen
– *Nein:* Klage erheben, Meldung an EDÖB oder kantonalen Datenschutzverantwortlichen

7. Gibt es eine gesetzliche Grundlage, um die Geobasisdaten zu bearbeiten?

– *Ja:* weiter bei Frage 8
– *Nein:* keine Bearbeitung

8. Erlaubt die gesetzliche Regelung die Veröffentlichung der Geobasisdaten?

– *Ja:* weiter bei Frage 9
– *Nein:* keine Veröffentlichung – Bearbeiten für interne Zwecke (Planung) ist zulässig; weiter bei Frage 13

9. Sind die Zugangsvoraussetzungen erfüllt?

– *Ja:* Geobasisdaten können im Rahmen des gesetzlich zugelassenen Umfangs bezogen und verwendet werden; weiter bei Frage 10
– *Nein:* Zugang zu Geobasisdaten ist nicht möglich; weiter bei Frage 13

10. Verstösst das Bearbeiten von Daten durch die öffentliche Hand gegen verfassungsmässige Grundrechte?

– *Ja:* Unrechtmässigkeit im konkreten Fall; weiter bei Frage 13
– *Nein:* weiter bei Frage 11

11. Sind die Eingriffe in die Privat- oder Persönlichkeitssphäre verhältnismässig?

– *Ja:* Bearbeiten ist im beantragten Rahmen möglich; weiter bei Frage 12
– *Nein:* Bearbeiten im beantragten Umfang nicht möglich

12. Sind Sperrungsmöglichkeiten vorhanden?

– *Ja:* Zugang im Einzelfall beschränkt; weiter bei Frage 13
– *Nein:* Datenzugang ist umfassend möglich

13. Bin ich mit der Zugangsbeschränkung einverstanden?

– *Ja:* keine weiteren Folgen
– *Nein:* Verwaltungs- bzw. Verwaltungsgerichtsbeschwerde, evtl. Meldung an Beauftragten (des Bundes bzw. des Kantons)