Auszug aus Daniel Hürlimann/Daniel Kettiger (Hrsg.), Anonoymisierung von Urteilen, Helbing und Lichtenhahn, Basel 2021, S. 21-30

Anonymisierung: Rechtliche Aspekte

Daniel Kettiger

Mag. rer. publ., Rechtsanwalt
Berater und Anwalt in Thun, externer Projektleiter und Forschungskoordinator am Kompetenzzentrum für Public Management (KPM) der Universität Bern

Inhaltsverzeichnis

1. Datenschutzrechtlicher Kontext

1.1 Personendaten als Ausgangspunkt

Die Anonymisierung von Gerichtsurteilen ist immer in einem datenschutzrechtlichen Kontext zu sehen. Zweck des Datenschutzes ist der Schutz von natürlichen und juristischen Personen vor missbräuchlicher Bearbeitung der sie betreffenden Daten. Art. 13 Abs. 2 BV[1] verankert das Recht auf Datenschutz unter dem Titel «Schutz der Privatsphäre» ausdrücklich, aber in eher genereller Weise als Grundrecht:[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Ein Teil der Lehre und Rechtsprechung leitet aus Art. 13 Abs. 2 BV auch einen grundrechtlichen Anspruch auf ein informationelles Selbstbestimmungsrecht ab.[3] 1

1 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.
2 Ausführlich zu Art. 13 Abs. 2 BV Belser, Rz. 56 ff., S. 349 ff.
3 Vgl. Belser, Rz. 115 ff., S. 375 ff.

2 Gegenstand des Datenschutzes sind *Personendaten*, d.h. alle Angaben, die sich *auf eine bestimmte oder bestimmbare Person beziehen* (Art. 3 Bst. a DSG[4]).[5] Darunter sind alle Daten zu verstehen, die Rückschlüsse auf eine Person erlauben, unabhängig davon, ob es sich um Tatsachen (Fakten) oder um Werturteile handelt und unabhängig von der Art der Information (Zeichen, Wort, Bild, Ton) oder vom Datenträger (Papier, Film, elektronische oder optoelektronische Datenträger, etc.). Entscheidend ist einzig, dass sich die Daten *einer oder mehreren Personen zuordnen lassen*.[6]

3 Die das europäische Datenschutzrecht bestimmende DSGVO regelt den Begriff der Personendaten, dort als «personenbezogene Daten» bezeichnet, etwas ausführlicher wie folgt (Art. 4 Ziff. 1 DSGVO[7]):

> *«‹personenbezogene Daten› alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‹betroffene Person›) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.»*

1.2 Das Kriterium der Bestimmbarkeit

4 Massgeblich, ob es sich um datenschutzrelevante Personendaten handelt, ist mithin die Bestimmtheit oder Bestimmbarkeit, d.h. die Möglichkeit, die betreffende Information einer bestimmten Person zuordnen zu können. Nach der bundesgerichtlichen Praxis ist eine Person «dann bestimmt, wenn sich aus der Information selbst ergibt, dass es sich genau um diese Person handelt».[8] Zur Bestimmbarkeit hat das Bundesgericht folgendes ausgeführt:

> *«Bestimmbar ist die Person, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor (BBl 1988 II 444 f. Ziff. 221.1). Die Frage ist abhän-*

4 Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1. Das vom Parlament am 25. September 2020 beschlossene neue Bundesgesetz über den Datenschutz (nDSG; BBl 2020 7639) definiert die Personendaten grundsätzlich in gleicher Weise, beschränkt den Begriff aber auf natürliche Personen (Art. 5 Bst. a nDSG).

5 Vgl. Gerschwiler et al., Rz. 3.27; Blechta, Rz. 4.

6 Ausführlich dazu Rudin, Rz. 10 ff.; Blechta, Rz. 7 ff.

7 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

8 Vgl. BGE 136 II 508, E. 3.2.

gig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat.»[9]

Diese Praxis kann an folgenden Beispielen veranschaulicht werden: 5

- *Bestimmte Person:*
  a. Xavier Muster, geb. 07.05.1960, von Trubschachen BE
- *Bestimmbare Person:*[10]
  a. «Sekretär der Geschäftsprüfungskommission der Stadt Burgdorf»
  b. «Oberstufenlehrer im Schulhaus Wäckerschwend»
  c. «… ein bekannter Burgdorfer Anwalt …»
  d. «AHV-IV Nr. 756.8293.5974.07»
  e. «Eigentümer Burgdorf-Gbbl. Nr. 2994-9»
  f. IP-Adresse

Das Bundesgericht hielt in seinem Leiturteil (dem sog. Logistep-Urteil) fest, dass *IP-Adressen* in bestimmten Fällen Personendaten darstellen und es genügt, dass die die betreffende Person auf der Grundlage der IP-Adresse erst durch das Tätigwerden der Strafverfolgungsbehörden bestimmt werden kann.[11] Das Bundesgericht ist dieser Auffassung, obwohl es selber eingesteht, dass in vielen Fällen die betreffende Person nicht ausfindig gemacht werden kann, so insbesondere dann, wenn verschiedene Personen zu einem Computer oder einem Netzwerk Zugang haben; es ist jedoch der Auffassung es genüge, «dass die Bestimmbarkeit in Bezug auf einen Teil der von der Beschwerdegegnerin gespeicherten Informationen gegeben ist».[12] Der Verfasser ist weiterhin der Auffassung, IP-Adressen seien in der Regel wegen der fehlenden Bestimmbarkeit der Person, welche das betreffende Endgerät wirklich besitzt und/oder nutzt, keine Personendaten.[13] 6

Sachdaten können Personendaten sein, wenn ein Bezug von der Sache zu einer Person besteht. Da jedes Grundstück eine Eigentümerin bzw. einen Eigentümer und jedes Motorfahrzeug eine Halterin bzw. ein Halter haben, gelten *Grundstückdaten* (z.B. ein Grundbuchauszug) und *Informationen über Motorfahrzeuge* grundsätzlich als Personendaten. 7

9 BGE 136 II 508, E. 3.2.
10 Vgl. auch Beispiele bei Gerschwiler et al., Rz. 3.31.
11 Vgl. BGE 136 II 508, E. 3.5.
12 Vgl. BGE 136 II 508, E. 3.5.
13 Vgl. Kettiger, Rz. 20.

8 Der für die Bestimmung einer Person zu betreibende Aufwand gilt in der Rechtspraxis dann als nicht mehr vertretbar und die entsprechenden Daten demzufolge nicht mehr als Personendaten, wenn nach den allgemeinen Lebenserfahrungen nicht mehr damit gerechnet werden muss, dass eine Interessentin oder ein Interessent diesen Aufwand auf sich nehmen wird (etwa durch komplizierte Auswertungen, Statistiken oder Analysen).[14] Bezüglich der *Anonymisierung von Urteilen* gelten nach einer älteren, aber bisher nicht widerrufenen Praxis der vormaligen Eidgenössischen Rekurskommission für Staatshaftung[15] allerdings weniger strenge Anforderungen: Die Anonymisierung ist genügend, wenn der Aufwand zur Feststellung der Identität des Beschwerdeführers so gross erscheint, dass ihn ein Dritter, der an den Angaben interessiert ist, vernünftigerweise nicht auf sich nehmen wird.[16] Es liegt überdies keine Verletzung des Anonymisierungsgrundsatzes vor, wenn Personen, welche mit den Einzelheiten des Falles vertraut sind, gegebenenfalls trotz Verschleierung erkennen können, um wen es geht.[17] Letzteres wurde vom Bundesgericht in einem anderen Fall bestätigt; dieses führte in diesem Zusammenhang folgendes aus:

> *«Eine Anonymisierung, wie immer sie ausgestaltet ist, schliesst nie aus, dass Verfahrensbeteiligte durch Recherche ausfindig gemacht werden können. Der mit der Anonymisierung angestrebte Persönlichkeitsschutz ist in der Regel gewährleistet, wenn Zufallsfunde durch beliebige Unbeteiligte vermieden werden.»*[18]

9 Diese Praxis bezüglich der Anforderungen an die Anonymisierung von Urteilen ist nach Auffassung des Verfassers zu überprüfen. Entweder besteht die Anforderung, ein Urteil zu anonymisieren bzw. pseudonymisieren, und dann hat dies lege artis zu erfolgen, d.h. nach dem Stand der aktuellen Technik, oder es wird auf eine Anonymisierung verzichtet.

2. Der Begriff der Anonymisierung

10 Der Begriff «anonym» meint ungenannt, ohne Namensnennung.[19] Er stammt ab vom spätlateinischen «anonymus», abgeleitet aus dem griechischen «anṓnymos» (an- = nicht, un- und ónoma [ónyma] = Name). Anonymität bedeutet, dass eine Person oder eine Gruppe nicht identifiziert werden kann.[20] Synonyme sind: inkognito, unbekannt, verdeckt, namenlos.

11 Für den Begriff der «Anonymisierung» findet sich weder in der DSGVO, im DSG, im nDSG noch im kantonalen Recht eine Legaldefinition. Der Einzige Anhaltspunkt findet

14 Vgl. Gerschwiler et al., Rz. 3.30; Rudin, Rz. 10.
15 Vgl. Entscheid HRK 2005-004 der Eidgenössischen Rekurskommission für die Staatshaftung vom 15. Februar 2006, VPB 70.73 vom 15. Februar 2006.
16 Vgl. Entscheid HRK 2005-004 (Fn. 15), E. 5b, c.
17 Vgl. Entscheid HRK 2005-004 (Fn. 15), E. 5d/bb.
18 Urteil 2E_1/2013 des Bundesgerichts vom 4. September 2014, E. 4.3.4.
19 Quelle: Wikipedia.
20 Quelle: Duden.

sich im Luzerner Datenschutzrecht (§ 4 Abs. 5 DSG LU[21]): «… sind Personendaten so zu anonymisieren, dass die betroffene Person nicht mehr bestimmt oder bestimmbar ist.» In ähnlicher Weise wird die Anonymisierung in den Erwägungen zur DSGVO beschrieben:

> «*Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.*»[22]

Anonymisierung bedeutet demnach die Verwischung bzw. Unterbrechung der Bestimmbarkeit einer Person, so dass diese nicht bzw. nicht mehr identifiziert werden kann. 12

3. Abgrenzung zur Pseudonymisierung

3.1 Theorie

Für die Peseudonymisierung besteht im schweizerischen Recht ebenfalls keine Legaldefinition. Demgegenüber definiert die DSGVO die Pseudonymisierung wie folgt (Art. 4 Ziff. 5 DSGVO): 13

> «*die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.*»

Im Gegensatz zur Anonymisierung stellt mithin die Pseudonymisierung einen reversiblen Akt dar; mit der vom Pseudonym getrennten Information ist eine Re-Identifizierung möglich. 14

3.2 Praxis (Beispiel)

Peter hat folgende Tabelle, welche Informationen zu Personen und damit Personendaten enthält: 15

ID	*Vorname*	*Nachname*	*Krankheit*	*Behandlung*
0001	Susi	Meyer	Brustkrebs	Operation

21 Gesetz über den Schutz von Personendaten (Datenschutzgesetz, DSG) vom 02.07.1990, SRL 38.

22 Erwägungsgrund 26 zur DSGVO.

16 Peter möchte seine Tabelle *anonymisieren*. Er löscht die Spalten «Vorname» und «Nachname» und erhält eine anonymisierte Tabelle, denn die Informationen sind nur noch der ID, nicht aber der betreffenden Person zuzuordnen:

ID	*Krankheit*	*Behandlung*
0001	Brustkrebs	Operation

17 Peter möchte seine Tabelle *pseudonymisieren*. Er gibt jedem Datensatz in seiner Tabelle eine ID. Dann speichert er in einer zweiten Tabelle die jeweilige ID, den Vornamen und den Nachnamen. Aus der ersten Tabelle löscht er nun die Spalten «Vorname» und «Nachname».

Erste Tabelle		
ID	*Krankheit*	*Behandlung*
0001	Brustkrebs	Operation

Zweite Tabelle		
ID	*Vorname*	*Nachname*
0001	Susi	Meyer

18 In der ersten Tabelle sind nun die Informationen pseudonymisiert; ohne Hilfe der zweiten Tabelle können die Informationen in der ersten Tabelle mit keiner Person verknüpft werden. Solange es aber die zweite Tabelle gibt, sind die Informationen nicht anonym, den mittels der zweiten Tabelle kann jederzeit ohne weiteres ein Bezug zwischen der Sachinformation und einer bestimmten Person hergestellt werden. Die datenschutzrechtlich geforderte Bestimmbarkeit wird durch die ID gewährleistet, welche die Informationen beider Tabellen verknüpft. Die gleiche Situation haben wir, wenn ein «anonymisiertes» Gerichtsurteil im Internet veröffentlicht wird und die Verfahrensnummer trägt (z.B. ein Bundesgerichtsurteil mit einer Verfahrensnummer im Stil von 2E_1/2013, welche in sich auch noch gleich kodierte Information über Abteilung und Verfahrensart enthält). Über die Verfahrensnummer und die Geschäftsverwaltung ist jederzeit eine Re-Identifizierung möglich.

4. De-Anonymisierung

4.1 Erkennungsmerkmale

19 Eine De-Anonymisierung (auch etwa Re-Identifizierung) beruht immer auf Erkennungsmerkmalen, die alleine oder in Verbindung mit weiteren Erkennungsmerkmalen die Bestimmung der betreffenden Person ermöglichen. Die De-Anonymisierung durch Abgleich mit anderen Urteilen oder anderen (auch justizfernen Datenbanken)[23] wurde in anderen Publikationen auch schon «Linkage-Methode» (zu Deutsch: Methode der Verknüpfung) genannt.[24]

23 Siehe dazu gleich unten Ziff. 4.2.

24 Vgl. Vockinger/Mühlematter.

Erkennungsmerkmale (in Verfahren des Natural Language Prozessing als «named entities» bezeichnet) können sich direkt auf die betreffende Person beziehen oder sie können weitere Personen, Orte oder Sachen betreffen, die mit der betreffenden Person im Urteil und allenfalls eben auch in anderen Datensammlungen in einem bestimmten Zusammenhang stehen. 20

- *Beispiele personenbezogener Erkennungsmerkmale:*
  a. Name und Vorname[25]
  b. Spitzname (nickname)
  c. Geschlecht
  d. Geburtsdatum
  e. AHV-Nummer
  f. Körpergrösse und andere biometrische Daten
  g. Berufstitel (z.B. MA, MLaw, Dr.)
  h. ausgeübte Berufe, z.B. Autoverkäufer, Apothekerin
  i. berufliche Funktion, z.B. Abteilungsleiterin
- *Beispiel anderer Erkenungsmerkmale*
  a. personenbezogene Erkennungsmerkmale anderer Personen im Verfahren (Richter/innen, Anwältinnen bzw. Anwälte, Zeuginnen bzw. Zeugen, etc.)
  b. geografische Namen, z.B. Wohnorte, Postleitzahlen, Unfallorte
  c. Namen von Unternehmen und Institutionen (z.B. Museen)
  d. Treffpunkte (Restaurants, etc.)
  e. Informationen zu (Motor-)Fahrzeugen, z.B. Marke, Kennzeichen, etc.
  f. Informationen betreffend Freizeitaktivitäten
  g. Informationen betreffend Reiseaktivitäten (Reise, Autofahrt, Wanderung), allenfalls mit Angabe von … nach.
  h. UID-Nummer
  i. IP-Adresse

Erkennungsmerkmale können je nach Kontext eines Urteils und Anzahl am Verfahren beteiligte Personen eine unterschiedliche Unterscheidungskraft aufweisen. Darauf wurde in einem älteren Urteil wie folgt hingewiesen: 21

> *«… publizierten Merkmale weisen eine unterschiedliche Unterscheidungskraft auf.» […] «… wirkt der Titel (…) in der Bundesverwaltung nicht allzu unterscheidend, da es*

25 Name und Vorname führen nicht zwangsläufig zu einer Identifizierung, da es oft mehrere, ja tauende von Personen mit gleicher Namen-Vornamen-Kombination gibt.

viele Mitarbeitende mit diesem Titel gibt.» […] «Am stärksten individualisierend wirkt das Merkmal der Zugehörigkeit zur Einheit Z., weil diese aus einer relativ kleinen Anzahl von Personen bestand.»[26]

22 Oft können aber schon zwei bis drei Erkennungsmerkmale genügen, um mittels einer einfachen Suche in der Suchmaschine Google im Internet eine Person ausfindig zu machen bzw. eindeutig zu bestimmen:[27]

- Die Verknüpfung eines gängigen Frauen-Vornamens + «Zürich» + «Logopädin» führte zu Name und Adresse der Person.
- Die Verknüpfung «Esther Joy» + «Zimmerwald» führte zu Name und Adresse der Person.

23 Nicht unterschätz werden darf die Unterscheidungskraft von *geografischen Namen* wie Strassen, Ortschaften und Gemeinden (hier bezogen auf die Schweiz):[28]

- «Länggassstrasse» gibt es nur in Bern und Nottwil.
- «Hühnerbühl» gibt es als Flurbezeichnung mehrmals, «Hühnerbühlrain» als Strassennamen nur in Bolligen.
- «Rougemontweg» gibt es nur in Bern, Hünibach und Thun (die Adresse «Rougemontweg 2a» nur in Thun).
- «Wegmühle» gibt es in der Schweiz als Flur- und Ortsbezeichnung nur ein Mal, in Bolligen.

4.2 Spezifische Datenbanken und Such-Tools

24 Es bestehen eine Menge von besonderen Datenbanken – teilweise mit eigenen Such-Tools, teilweise für Google-Abfragen zugänglich – die Verzeichnisse über Erkennungsmerkmale enthalten. Einige Beispiele seien hier erwähnt:

- Telefonverzeichnisse;
- UID-Register;
- Handelsregister;
- amtliches Verzeichnis der Strassennamen;
- amtliches Verzeichnis der Ortschaftsnamen (inkl. Postleitzahl);
- amtliches Gemeindeverzeichnis;
- interaktive Karten mit weiteren geografischen Informationen (z.B. Grundstücksnummern oder EGRID);
- private Verzeichnisse mit Todesanzeigen;

26 Auszüge aus dem Entscheid HRK 2005-004 (Fn. 15).
27 Ergebnisse von Versuchen des Verfassers im Januar 2019.
28 Ergebnisse von Recherchen des Verfassers.

Nicht alle dieser Datenbanken sind direkt im Internet verknüpfbar. Teilweise lassen sich aber die betreffenden Daten herunterladen oder «crawlen» und können dann in einer lokalen Datenbank verknüpft werden. 25

4.3 Einmal im Web – immer im Web

Personendaten aus Gerichtsurteilen, die einmal im Internet öffentlich zugänglich waren, bleiben dies teilweise auch dann, wenn sie nachträglich anonymisiert werden. Grund dafür ist, dass die im Internet publizierten Urteile von Privaten ziemlich rasch kopiert bzw. «gecrawlt» und dann in privaten, aber öffentlich zugänglichen Datenbanken zugänglich bleiben. Dies sei am nachfolgenden Beispiel illustriert. 26

Das Urteil 1C_257/2015 des Bundesgerichts vom 29. September 2015 wurde vom Bundesgericht zuerst – entsprechend seinen Anonymisierungsregeln regelkonform – nicht-anonymisiert im Internet veröffentlicht, nach rund vier Tagen aber auf Antrag des Anwalts des Beschwerdeführers nachträglich anonymisiert. In der öffentlich zugänglichen Urteilsdatenbank des Bundesgerichts[29], die auch bei entsprechenden Abfragen in Google erscheint, ist das Urteil heute bezüglich der Person des Beschwerdeführers anonymisiert. Auch die im Rahmen des Projekts «Deutschsprachiges Fallrecht (DFR) «gecrawlte» Fassung des Urteils auf dem Server der Universität Bern ist anonymisiert.[30] Auf der vom Verein «PolyReg Allg. Selbstregulierungs-Verein»[31] betriebenen, ebenfalls frei zugänglichen Internet-Sammlung der Bundesgerichtsurteile erscheint demgegenüber der Name des Beschwerdeführers ohne Anonymisierung.[32] Über das Portal entscheidsuche.ch findet man im Übrigen gleichzeitig auch das Urteil der Vorinstanz; dieses ist allerdings bezüglich des Namens des Beschwerdeführers anonymisiert. 27

5. These

Zum Schluss kann die folgende *These* formuliert werden: Rein (datenschutz-)rechtlich betrachtet ist eine Anonymisierung von Entscheiden und Urteilen nur eine *Pseudonymisierung*, solange die Urteils- bzw. Verfahrensnummer bleibt. 28

Dies bedeutet, dass man es in den meisten Fällen von so genannt anonymisierten Urteilen nur mit pseudonymisierten Urteilen zu tun hat. Und wenn das Gericht parallel zur Publikation des pseudonymisierten Urteils mit Verfahrensnummer im Internet auch das nicht-anonymisierte Urteil im Gerichtsgebäude für einige Tage öffentlich auflegt, wie dies beispielsweise das Bundesgericht tut, dann ist die De-Anonymisierung bzw. Re-Identifikation nicht nur durch das Gericht, sondern auch durch aussenstehende Dritte möglich – allerdings mit einem nicht unerheblichen Aufwand. Erst dann, wenn ein 29

29 Rechtsprechung (gratis), weitere Urteile ab 2000.

30 https://www.servat.unibe.ch/dfr/bger/2015/150929_1C_297-2015.html.

31 http://www.polyreg.ch/

32 http://www.polyreg.ch/bgeunpub/Jahr_2015/Entscheide_1C_2015/1C.297__2015.html

Urteil in anonymisierter Form ohne die ursprüngliche Verfahrensnummer veröffentlicht wird (beispielsweise in einer Sammlung von Leitentscheiden, die fortlaufend nummeriert werden), liegt eine Anonymisierung im Wort- und Rechtssinn vor.

Literatur

Belser, Eva Maria, § 6 Der grundrechtliche Rahmen des Datenschutzes, in: Belser, Eva Maria/Epiney, Astrid/Waldmann, Bernhard (Hrsg.), Datenschutzrecht, Bern 2011, S. 319–410

Blechta, Gabor P., BSK DSG, 3. Aufl., Basel 2014, Art. 3

Gerschwiler, Stefan et al., Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Passadelis, Nicolas/Rosenthal, David/Thür, Hanspeter, Datenschutzrecht, Basel 2015, S. 73–88

Kettiger, Daniel, Rechtliche Rahmenbedingungen für Location Sharing Systeme in der Schweiz, Jusletter vom 9. August 2010

Rudin, Beat, SHK Datenschutzgesetz, Bern 2015, Art. 3

Vockinger, Kerstin Noëlle/Mühlematter, Urs Jakob, Re-Identifikation von Gerichtsurteilen durch «Linkage» von Daten(banken), Jusletter 2. September 2019