The impact of losing control over personal information from Big Brother to Big Data

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieurin

in

Business Informatics

by

Michaela Jungwirth BSc.
Registration Number 0926035

to the Faculty of Informatics
at the Vienna University of Technology

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, 20th April, 2015

Michaela Jungwirth

Markus Haslinger

Declaration of Authorship

Michaela Jungwirth BSc.
Mitterweg 27, 4120 Neufelden

I hereby declare that I have written this Diploma Thesis independently, that I have completely specified the utilized sources and resources and that I have definitely marked all parts of the work - including tables, maps and figures - which belong to other works or to the internet, literally or extracted, by referencing the source as borrowed.

Vienna, 20th April, 2015

Michaela Jungwirth

Danksagung

An dieser Stelle möchte ich all jenen danken, die durch ihre fachliche und persönliche Unterstützung zum Gelingen dieser Arbeit beigetragen haben.

Mein Dank gilt Herrn. Prof. Dr. Markus Haslinger für die Unterstützung sowie die sprachliche und inhaltliche Verbesserung meiner Arbeit.

Besonderer Dank gilt meiner Familie, insbesondere meinen Eltern, die mir mein Studium ermöglicht und mich in all meinen Entscheidungen unterstützt haben.

Abstract

The processing of personal data in numerous Web 2.0 platforms, mostly willingly divulged by users as well as the legal impacts on European level and especially in Austria were decisive for the choice of my topic.

This paper aims to demonstrate legal and social impacts when losing control over personal information of private persons. As already enshrined in the title of my master thesis, the time period for my research starts at the era of Big Brother in the 1970's up to now, which is called the era of Big Data. The first two chapters include all definitions, which form the basis of my research. To understand the development and features of Big Data, these chapters include definitions of privacy, data protection and personal data.

My thesis also covers the development of society in conjunction with the enactment of applicable Austrian laws, as well as regulations and directives of the European Union concerning data protection of personal information. Besides that, the existing data protection mechanisms and approaches are taken into account. In this context the Austrian Data Protection Act is an important source of information. However, since these legal conditions are partially outdated, I pointed out obsolete and insufficient parts.

Furthermore, I paid particular attention to personal data used in cloud computing, web-tracking, video surveillance and Big Data. In order to establish a connection to the real life examples, I also concentrated on "Hot topics". Finally, I published my research results in a blog, to open the social development and the current legal situation in a clear and understandable way to the public.

Kurzfassung

Der rasante Anstieg von Web 2.0 Plattformen, die eine Vielzahl an großteils bereitwillig preisgegebenen personenbezogenen Daten von Nutzerinnen und Nutzern verarbeiten sowie die rechtlichen Einflüsse auf europäischer Ebene und in Österreich, waren ausschlaggebend für die Wahl meines Diplomarbeitsthemas.
Zielsetzung dieser Arbeit ist es, die sozialen und rechtlichen Implikationen, die der Kontrollverlust von persönlicher bzw. personenbezogener Information mit sich bringt, aufzuzeigen. Zum besseren Verständnis widme ich mich zu Beginn der historischen Entstehung des Datenschutzes und der Erklärung einiger fundamentaler Begriffe in diesem Zusammenhang.

Diese Arbeit beinhaltet neben der Analyse dieser gesellschaftlichen Entwicklung auch rechtliche Aspekte, sowie eine Darlegung existierender Datenschutzmechanismen sowie der Ansätze zur Vereinheitlichung des Datenschutzniveaus. Relevante Ausschnitte aus Richtlinien und geplanten Verordnungen der Europäischen Union, den Datenschutz betreffend, werden diskutiert. Eine wichtige Informationsquelle für die Erstellung dieser Arbeit ist das österreichische Datenschutzgesetz 2000, kurz DSG 2000. Besondere Beachtung widme ich der Nutzung von personenbezogenen Daten in den Bereichen Cloud Computing, Web-Tracking, Videoüberwachung und Big Data. Um die Verbindung zu den realen Fällen, die gemeinsam mit einer Staatsanwältin erarbeitet wurden, zu schaffen behandle ich in einem eigenen Kapitel auch besonders aktuelle Themen des Kontrollverlusts von persönlicher Information. Aufgrund der AktualitÃďt meines Diplomarbeitsthemas und des "Hinterherhinkens"der Gesetzgebung ist die Auswahl meiner Quellen im Literaturverzeichnis breit gefächert.

Ich veröffentliche meine Forschungsergebnisse nach und nach in einem Blog, um auch der breiten Öffentlichkeit den Zugang zu der analysierten sozialen Entwicklung und der aktuellen rechtlichen Situation zu ermöglichen.

Contents

Abbreviations

ABGB	Allgemein Bürgerliches Gesetzbuch
ARGE	Arbeitsgemeinschaft
ASP	Application service provider
BGBI	Bundesgesetzblatt
BIC	Business Identifier Code
BIM	Ludwig Boltzmann Institut für Menschenrechte
B2B	Business-to-Business
B2C	Business-to-Consumer
CID	Criminal Investigation Department
COPA	Child Online Protection Act
COPPA	Children’s Online Privacy Protection Act
DNT	Do Not Track
DPPA	Drivers Privacy Protection Act
DSG	Datenschutzgesetz
DSRL	Datenschutzrichtlinie
ECJ	European Court of Justice
ECPAT	End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes
ELGA	elektronische Gesundheitsakte
ENISA	European Network and Information Security Agency
EU	European Union
EEA	European Economic Area
FERPA	Family Educational Rights and Privacy Act
FTC	Federal Trade Commission
GB	Gigabyte
GLBA	Gramm-Leach-Bliley Act
GPS	Global Positioning System
HTML	Hyper Text Markup Language
IBAN	International Bank Account Number
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IRI	Institut für Rechtsinformatik der Leibniz Universität Hannover
ISPA	Internet Service Provider Austria
JGG	Jugendgerichtsgesetz
MB	Megabyte
NDC	National Data Center
NGO	Non Governmental Organisation
NIST	National Institute of Standards and Technology

OECD	Organisation for Economic Co-operation and Development
ÖIAT	Österreichisches Institut für angewandte Telekommunikation
TB	Terabyte
PT	Petabyte
SIT	Fraunhofer-Institut für Sichere Informationstechnologie
SLA	Service Level Agreement
SMS	Short Message Service
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TAN	Transaktionsnummer
TEU	Treaty on European Union
TKG	Telekommunikationsgesetz
TPL	Tracking Protection List
UAV	Unmanned Aerial Vehicles
UIDH	Unique Identifier Header
WLAN	Wireless Local Area Network
W3C	World Wide Web Consortium

"Datenschutz ist digitaler Umweltschutz"

Jan Philip Albrecht

"If you have enough metadata, you don't really need the content"

Stewart Barker, 2014

CHAPTER 1

Historical development of data protection

1.1 The Right to Life

In 1890 Samuel Warren and Louis Brandeis published one of the most important articles in history of American law, namely "The Right to Privacy", in the Harvard Law Review. [2] They pointed out that an individual shall have full protection in person and in property. Almost more important than the former statement is their observation that it is necessary to define anew the exact nature and extent of such protection from time to time, because of a result of political, social and economic changes [3]. Originally the "Right to Life" gave a remedy only for physical interference with life and property, whereas later the right to life is expanded through recognition of the legal value of sensations. The following parts of the article in Harvard Law Review deal with the extension and development of the right to life law concerning life and property. Due to expanding the concept of property from protecting not only tangible property but also intangible property the growth of the legal conception of property took place similarly to the expansion of the right to life. Recent inventions and business methods, like instantaneous photography and newspapers, made it desirable and foremost necessary to adapt the common law [4].

Warren and Brandeis said also in their article that the press is overstepping the obvious bounds of propriety and decency in every direction. Gossip became a trade asset and for satisfaction of curiosity details of sexual relations were spread in daily newspapers. These examples showed that salitude and privacy had become more and more important for an individual [5]. An essential part in this article is the following statement of the

[2] [Sim96], p.215–241

[3] [Rig]

[4] [Sam90]

[5] [Sam90]

authors: "It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is." [6]

Next, the authors have investigated if the law of slander and of libel covers not only material rights, but also spiritual ones. They concluded that the common law is insufficient to protect the privacy of an individual, because the law of defamation deals only with damage to reputation [7].

The following paragraphs were dedicated to the intellectual property, especially the right to prevent the publication of manuscripts or works of art. Each individual could determine, whether their thoughts, sentiments, and emotions were communicated to others or not. For clarification and better understanding, Warren and Brandeis gave concrete examples, when applying intellectual property right rightly. Once more the authors have examined if the principles of the intellectual property law protected the privacy of an individual, too [8]. The discussion occupied more than two pages and in conclusion Warren and Brandeis said "that the protection afforded through thoughts, sentiments, and emotions expressed though the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone." [9]

The right of property, which inheres the quality of being owned or processed, formed the basis of the right to prevent publication. Strictly speaking the right of property only protected the right of the creator concerning any profits, which could have been derived from the publication. They also mentioned that the principle of an inviolate personality, especially the protection of personal writings and all other personal productions, against publication in any form, but not against theft and physical appropriation, is not the same as the principle of private property. [10] If Warren and Brandeis' conclusion was correct, then "the existing law affords a principle from which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewarding or reproducing scenes or sounds. In contrast to cases worth being protected where any particular medium or form of expression had been adopted, the protection of products of intellect were confined by the authorities." [11]

Before I elaborate on the considered limitations of the right to privacy, I want to point out Warren and Brandeis' recommendation to base the right to privacy on the jurisdictional justifications [12]. In their article they state that "in some instances where protection has been afforded against wrongful publication, the jurisdiction had been asserted, not on the ground of property, or at least not wholly on that ground, but upon

[6] [Sam90]

[7] [Sam90]

[8] [Sam90]

[9] [Sam90]

[10] [Sam90]

[11] [Sam90]

[12] [Sam90]

the ground of an alleged breach of an implied contract or of a trust or confidence." [13]

Finally the authors acknowledged that an exact definition of this new theory is a difficult task, hence they considered the limitations and remedies of this right of privacy as follows:

- "The right to privacy does not prohibit any publication of matter which is of public or general interest." [14]
- "The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel." [15]
- "The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage." [16]
- "The right to privacy ceases upon the publication of the facts by the individual, or with his consent." [17]
- "The truth of the matter published does not afford a defence." [18]
- "The absence of "malice" in the publisher does not afford a defence." [19]

To sum up one of the most influential essays in the history of American law, Warren and Brandeis stated that the data protection law must evolve in response to technological change. For sustaining the right to one's personality with respect to modern business practices and invasive inventions it is absolutely essential to develop legal remedies [20]. Moreover, future legislation should place greater emphasis on the privacy of the individual and bring criminal liability within narrower limits. [21] Warren and his co-author Brandeis also stated that "the protection of society must come mainly through a recognition of the rights of the individual. Each man is responsible for his own acts and omissions only." [22]

[13] [Sam90]
[14] [Sam90]
[15] [Mat14a]
[16] [Sam90]
[17] [Sam90]
[18] [Sam90]
[19] [Sam90]
[20] [Mat14a]
[21] [Sim96], p.215–241
[22] [Sam90]

1.2 Global debate on data protection

In his speech at Stanford University in 1975, President Gerald R. Ford referred to a "big brother bureaucracy", in which the privacy of citizens must be protected. The state in the figure of a "Big Brother" initially came up in debates on cameras and wiretaps. Those technical capabilities allegedly violated the personal privacy of citizens of the United States of America, so that politicians and the public debated intensively privacy issues in the 1960s and 1970s.

1.2.1 Nineteen Eighty-Four

The figure of a "Big Brother" originates from the novel *Nineteen Eighty-Four* and was originally used to point out potential dangers of databases. *Nineteen Eighty-Four* is considered in political discussion as a symbol for monitoring, although this is only a secondary aspect of this book. The author Eric Blair, who published the novel under the pseudonym George Orwell in 1949, tells the story of Winston Smith, who lives in a state called Oceania. This state is dominated by a single political party seeking control of the party members and residents in their thoughts to the world [23]. The "Thought Police" represents observation and repression of the inhabitants, whereas Big Brother plays as a guardian of revolution a rather mythical role and observes people with a penetrating gaze of coins, posters and books. The figure represents dictatorial rules, however, carries also religious-mythical traits [24]. With regard to monitoring theories, commentators referred to the novel *Nineteen Eighty-Four* in privacy debates in the 1960s. The technology developed faster than Orwell might have thought and his scenario appeared feasible quite soon from a technical point of view [25].

1.2.2 Plans for a national data center

In August 1966, the New York Times commented on plans for a National Data Center with the following headline: "The Orwellian nightmare would be brought very close indeed if congress permits the proposed computer NDC to come into being." [26] In a report of 1965 the Social Science Research Council recommended that the Bureau of Budget should standardize and merge data sets of federal agencies for statistical purposes. [27] For gaining insights into the social structure, proponents of this national data center hoped for fully effective political programs. [28] While proponents also referred to anonymous and aggregated statistics, critics feared an "effective end of privacy" by clustering of scattered information [29].

[23] [Neu14] p.73-74

[24] [Neu14] p.75

[25] [Neu14] p.77

[26] The New York Times 1966, p. 36

[27] [Neu14] p.77-78

[28] Harvard Law Review, p. 400 et seq.

[29] [Neu14] p.77-78

1.3 Origin of data protection term

The term "data protection", as it is used in the data protection act of Hessen, was originally understood as protection of data in terms of a backup against loss, alteration or theft. The current term "data protection", which is still valid until now was mentioned for the first time in Ulrich Seidel's essay "personality problems of the electronic storage of private data". [30] Seidel's dissertation "databases and personal rights" of 1972 treated the differentiation of substantive and formal data protection law.

1.4 World's first data protection act

In the mid-sixties of the last century, automated data processing in the public administration of the Federal Republic of Germany became more and more popular. Due to that fact contentious discussion about the threats posed by emerging databases of state authorities came up. Both the desire to protect the privacy of individuals and the fear that a comprehensive information power of the state could arise, led to the belief that the more and more effectively automated information processing required by public authorities needed to be restricted through data protection [31]. The enactment of the first data protection act in the world of Hessen in Germany in 1970 built up a landmark in the history of data protection [32]. The established legal framework secured the right of informational self-determination, in other words the right of an individual determining itself about the use and abandonment of personal data [33]. Electronically processed data must be protected from unauthorized access, competent authorities have to treat the personal data as confidential and affected people should have the possibility to rectify inaccurate data. It also determined the establishment of a data protection officer as an independent supervisory authority for the public authorities of the country [34].

1.5 Federal Data Protection Act of Germany

The Federal Data Protection Act of January 28, 1977 had also a strong focus on the protection of personal data and was determined by the basic idea that government agencies as well as companies may not interfere with the right of individuals to be let alone [35]. At that time privacy was considered as a protection of personal data against illegitimate data processing. Because of the introduction of the so called necessity principle, it was only allowed to process personal data, which was necessary for the fulfillment of the statutory duty of the authority; otherwise it was a misuse of personal data [36].

[30] New Legal Weekly 1970, S. 1581

[31] [fdDufdRaAB]

[32] [Gen04a]

[33] [Hes12]

[34] [fdDufdRaAB]

[35] [fdDufdRaAB]

[36] [Hes12]

1.6 Census verdict in 1983

The following caricature was drawn on the occasion of the German census in 1983 and represents a person, who participates as an individual in the census, but exists afterwards only as a simple number. A respected and esteemed citizen, who was up to 1983 an individual person would get a numbered citizen, whose personality would have no more importance to the state. Transparent citizens would be exploited by the German surveillance state through the planned, comprehensive data storage [37].

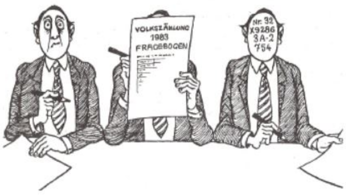

Figure 1.1: Caricature from 1983 [38]

In the focus of criticism there were insufficient data protection and the possible abuse of personal data. According to recommendations of the United Nations, censuses were conducted in many Western European countries in regular intervals of about ten years. At this time the next census in Germany should take place in 1981 and for this reason a new population census law had to be created. Due to financial problems it was not possible to adopt the law in 1981 and 1982. Once these problems had been solved, the German Bundestag was able to unanimously enact the population census law [39]. The decision of the Federal Constitutional Court of December 15, 1983 (census verdict) was a constitutional milestone ins strengthening the establishment of data protection. [40] The German highest court deduced from the constitutional general personal rights the right to informational self-determination in census verdict. [41]

[37] [Ber09]

[38] [Ber09]

[39] [Ber09]

[40] [Mar12], p.67-70

[41] BVergG v. 15.12.1983, BVerfG 65, 1ff

CHAPTER 2

Fundamental terms and theories

2.1 Definitions of privacy

Why are we thinking that privacy is worth protecting? Beate Rössler deals with such questions in her book "The value of privacy" and introduces different definitions of privacy depending on the context. Within our liberal democratic society autonomy is appreciated, but autonomy is not affordable without privacy protection and a distinction between private and public dimensions of life. Religion is my private matter, but what my clothes look like or which profession I have, too. At any level of privacy, persons want to keep control over personal data, decisions and the access to their apartments. Therefore, Beate Rössler defines something as private, if someone is entitled as well as able to control the access to personal data, accommodations, decisions and behavior [42]. On the one hand access can be understood in a metaphorically context, for instance appeals against decisions, but on the other hand access can be meant literally as for example the access to an accommodation. Privacy can be classified in three different dimensions [43]. First, the informational privacy deals with personal data and what others know about my private life. Second, private decisions and actions, like the selection of wardrobe or profession, are called "dezisionale" privacy. The third and last classification is the local privacy, which concerns the privacy within a person's accommodation. The habitat of individuals should be demarcated from the public and moreover offer possibilities for retreating of an individual [44].

Furthermore, Rössler explains the idea of privacy as a standard, which applies similarly to all persons, whether male or female. Privacy protects the freedom and autonomy of individuals. The protection of privacy is very important, because otherwise people cannot live freely and self-determined [45]. So, actually, what is the value of privacy?

[42] [Rös01]
[43] [Rös]
[44] [Rös01]
[45] [Rös]

Why is it that we cannot imagine a society without privacy, such as in George Orwell's book "1984"? The modern terms autonomy and self-determination serve as the basis for explanatory purposes. Everybody should be able to decide on the own lifestyle [46].

The examples given by the author demonstrate the recent data protection problem. First, she discusses the possible introduction of biometric data to the passport. Some people would argue that it does not matter, whether the passport lists apart from the eye color also the shape of the iris. The problem is not the possible violation of the informational privacy, but the more data is collected, the sooner personal data can be misused [47]. If the private autonomy is violated, the public autonomy of the democracy is also concerned. Potential conflicts between the necessary task of a state to protect this citizens against terrorism on the one hand and the protection of the individual freedom of citizens on the other hand can unfortunately not always be prevented. Indeed, for the limitation of the civil rights and liberty and of the autonomy there must be an important reason, like counter terrorism, but also a high degree of effectiveness when achieving objectives is promised [48].

The second example deals with the rapid development of information technologies which endangers the informational privacy. The problem thereby is the possibility of permanent observation, the identification and surveillance of an individual. Everyone surfing the internet pays by credit card and orders things and readily gives up areas of privacy [49].

The third example remains to be considered, which deals with the development of the media and telecommunication market, especially with the TV show "Big Brother". The participants of this show forego entirely on their privacy. In contrast to "Big Brother", persons affected of data collections of federal government as well as of confidential video surveillance are unaware of the fact that they are monitored. [50]

2.2 Definitions of data protection

The origin of the data protection term was already mentioned in *chapter Origin of data protection term on page 7.* In the Web 2.0 a multitude of personal data are processed, whereby the use of personal data offers on the one hand attractive benefits for customers as well as companies, but on the other hand lurking dangers should not be underestimated. In contrast to an individual usage of personal data, the combination and correlation of these data pose a great risk. In other words, the combination of personal data makes it possible to easily find out buying habits, personal interests, physical and mental condition, etc. Shopping in an online shop has both advantages and disadvantages. First, let us consider the advantages, starting with personalized accounts via recommendations, which are based on previous selections up to saving time and 24/7 availability. The creation of a suitable motion profile across a variety of websites is possible by introducing new technical

[46] [Rös01]

[47] [Rös01]

[48] [Rös01]

[49] [Rös]

[50] [Rös]

processes and represents only one disadvantage of this concrete example. This example is intended to show that the risks of divulging personal data are often underestimated. Therefore, the next paragraphs are concerned with the legal definition and demarcation of data protection.

The fundamental right of data protection is of course embodied in the Austrian Federal Act concerning the Protection of Personal Data (DSG 2000). According to Article 1 (1) of DSG 2000 everybody shall have the right to secrecy for personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is excluded when data cannot underlie the right to secrecy due to their general availability or because they cannot be traced back to the data subject. Elaborations concerning relevant definitions are discussed in detail in *chapter Definitions of personal data on page 12.* Article 1 (2) [51] regulates the use of personal data, whereas Article 1 (3) [52] establishes the rights of data subjects. As far as personal data is not used in the vital interest of a data subject or with his consent, restrictions of the right to secrecy are only permitted to safeguard mainly legitimate interests of another; especially in case of an intervention by a public authority the restriction shall only be permitted based on laws necessary for the reasons stated in Article 8 (2) of the European Convention on Human Rights [53]. Such laws may provide for the use of data, where the data need to be particularly protected, only to safeguard important public interests and they also must determine adequate safeguards for the protection of the confidential interests of data subjects. Even in the case of permitted restrictions the intrusion of citizen's fundamental right to privacy shall be carried out using only the least intrusive of all effective methods. According to Article 1 (3) [54] everybody is entitled to obtain information about the data processor, the origin of the personal data and for what purpose they are used, as well as to whom the data is transmitted. Furthermore, everyone has the right of rectifying incorrect data and the right to delete inaccurate data. These rights only apply if the personal data is intended either for automatically processed data or processing in structured manual files.

[51] DSG 2000
[52] DSG 2000
[53] Federal Law Gazette No. 210/1958
[54] DSG 2000

2.3 Definitions of personal data

Personal data means any information relating to an identified or identifiable natural or legal person. Some examples of natural persons' data are the name, sex, purchasing power or the internet browsing habits. In contrast to data of natural persons, the legal form, ownership and profits are among data of legal entities. Anonymous information, which cannot be assigned to anyone, is not protected. Moreover, the right to privacy is strictly personal and cannot be sold, inherited or otherwise transferred. It expires with the death of a person [55]. In terms of content data can be divided into three categories: sensitive data with maximum protection, data relating to criminal law with lower protection and all other data with a general level of protection. Concerning the definition of personal data, it is not necessary that the processor can determine the absolute and unique identity of the person, but it is sufficiently if it is at least possible for some other person. An example would be the social security number without knowing the name or residence of the person concerned. Contrary to the processor of the social security number, health insurance companies are able to find out remaining personal data. The distinction between directly and indirectly related personal data is essential, because rules on the processing of indirectly related personal data are facilitated. Sensitive data is highly protected information, whereas the distinction between ordinary and sensitive data takes place on the basis of content [56].

Personal data is defined in the Federal Act concerning the Protection of Personal Data (DSG 2000) as information related to data subjects who are identified or identifiable; data are "only indirectly related personal" for a controller, a processor or a recipient of a transmission, when the data is related to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means [57]. Definition of personal data in DSG 2000 includes several terms, which need to be explained in more detail. According to Article 2 (2) [58] sensitive data is defined as data, which relate to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health and sex life [59].

A controller is a natural or legal person, a group of persons or an organ of a territorial corporate body or rather the offices of these organs. Controllers decide alone or jointly with others about the use of personal data, without regard whether they use the data by themselves or commissioning on processors. They are also considered as controllers, if the authorized processors use personal data for producing a work, unless the processor is prohibited from the usage or the contractor has to decide autonomously on the basis of rules of law or codes of conduct.

[55] [Son10]
[56] [Son10]
[57] [Son10]
[58] DSG 2000
[59] [Son10]

Moreover, the already mentioned processor needs to be defined. According to Article 2 (5) [60] a processor is a natural or legal person, a group of persons or an organ of a federal, state and local authority or rather the offices of these organs, whereas they use the data only for commissioned work. Finally, data subject is a frequently used term in the data protection law and is defined as any natural or legal person or group of persons, whose data are processed.

A file is a structured collection of personal data that is accessible by at least one specific search criterion [61]. Card indexes and simple lists are also files, because electronic processing is not mandatory. Because of misleading definitions in the Directive it is very important to make a distinction between an additional internal structure and a purely external structure. A collection of paper files is externally due to the file number a structured collection, whereas a database seems to be unstructured, but the single data records are obviously structured. Therefore, a file is a collection of personal data with an outer order, where the context is searched through by at least one criterion.

A data application is nothing else than the sum of logically linked application steps, which are organised in order to reach a defined result. These application steps are either entirely or partially automatically processed, thus performed by machines and controlled by programs. The data processing is composed of different flexibly arranged actions, but must form a logical unit. Interestingly, the Austrian data protection law defines the processing of data differently than the EU Directive 2002/58/EC.

The data processing in the EU Directive is similar to the usage of personal data in the Austrian DSG 2000. In Austrian law the usage of personal data is further divided in data processing and data transmission and is related to any kind of data handling within an application. Data transmission is defined as the transfer of data to other recipients than the data subject, the controller or the processor, especially publishing the data as well as the usage of data for another application area of the controller. Because of the fact, that the data application is changed while transmissioning data, the disclosure of data to others for processing purposes and information of data subjects concerning their data is called transfer of data. According to Article 2 (11) [62] the surrendering of data is the transfer of data from a controller to a processor in the context of a commissioned work. Publication is one example of data transmission in the sense of law.

Data processing consists of a wide range of many different elements, like determining, collecting, storing, sorting, surrendering, comparing, modifying, linking, reproducing, querying, dispensing, using, locking, deleting and destroying or any other way of handling data, whereas the before mentioned data surrendering is excluded. There are no overlaps or further classes when defining data processing or data transmission, indeed any usage of data is either a transfer or a processing action. Data processing can be further structured

[60] DSG 2000

[61] Article 2 (6) DSG 2000

[62] DSG 2000

in determining relevant data and surrendering of data. First, data determination and gathering is the collection of personal data with the intention of using them in a data application. Although such data arise randomly and no determination takes place, the data is still protected. Second, the transfer of personal data from a controller to a processor is already mentioned in the paragraph above. I want to point out the difference between surrendering and transmissioning of data. When surrendering data a natural or legal person shall be instructed to carry out the processing of personal data instead of the controller.

CHAPTER 3

Legal basis of data protection on the European level

In the European Union, data protection is regulated in several legal sources. Before dealing with these legal sources, the difference between an EU regulation and an EU directive must be mentioned.

3.1 Difference between regulation and directive

On the European level the data protection is presently regulated in the data protection directive from 1995. However, a future data protection regulation is scheduled in the planned reform of the European law of data protection. Because of that fact I want to point out those two legal instruments, directive and regulation, and highlight some differences. Currently the 28 member states legislate their own laws based on the data protection directive from 1995. [63] The various levels of implementation of this EU directive have led to an unequal level of data protection. A regulation is an instrument which is legally binding for all EU member states and individuals in these states to guarantee exactly the same data protection standard after the realization of the data protection reform. In contrast to that, a directive is one of five legal acts provided by the European Union [64] and solely addressed to the Member States. Moreover, a directive is not directly applicable to citizens, but the national legislation is. It does not matter how the member states transform an overall goal into a legally binding law it is up to the national legislation. [65] Therefore, a directive must be clearly distinguished from a regulation, since a regulation as a legal act of the Union will have a direct effect on EU citizens and needs not to be transposed into national law. Furthermore, directives are

[63] [Alb12]

[64] [Art12]

[65] [Joh12], p.295

intended to harmonize legislation in all member states of the Union, whereas the degree of harmonization depends on the arrangement of each directive. [66] A decisive advantage of the planned regulation is that companies are no longer able to select the country with the lowest standard of data protection. Ireland, compared to other EU member states, has a comparatively low level of data protection; that is why the American company Facebook has the European company's headquarters there (apart from aspects of taxation). The reform proposal also intends that European standards of data protection are valid as soon as data relating to European citizens are effected, no matter where the company's headquarter is. [67]

3.2 Directive 1995/46/EC

In accordance with the provisions of the Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 [68], member states shall ensure the protection of fundamental rights and fundamental freedoms, in particular the protection of privacy of individuals with regard to the processing of personal data. The Data Protection Directive, which was adopted after many years of tough negotiations in 1995, is a privacy standard in the fourth generation. A detailed description of the four different generations of Data Protection in Europe and especially in Austria is provided in *chapter Data Protection Generations on page 33.* The overall goal of this Directive is to protect the right of privacy of individuals as well as other fundamental rights and freedoms in the automated and non-automated processing of personal data. [69] The Directive aims to allow unimpeded flows of personal data within the European Union/the European Economic Area. [70]

The EU Privacy Directive 95/46/EC requires companies planning to transfer data to countries outside the European Economic Area (EEA) to ensure an adequate level of data protection. Companies in the U.S. may secure their level of data protection individually by joining the U.S.- EU Safe Harbor Program (see *chapter Safe Harbor Agreement*).

3.2.1 History of the Data Protection Directive

The genesis of this directive lies far back in the past: In 1975 the European parliament drew up first resolutions [71], however, the first regulatory proposals were made by the European Union in 1990. [72] [73]

[66] [Ale12], p.296

[67] [Alb12]

[68] [Dir95]

[69] [Joh12], S.296

[70] cf. [Vik14]

[71] So bereits die erste Entschließung des Parlaments zum Schutz der Rechte des Einzelnen angesichts der fortschreitenden Entwicklung auf dem Gebiet der automatischen Datenverarbeitung, AB L.EG Nr.C 69 v. 13.3.1975

[72] [Hol02], p.4

[73] Vorschlag für eine RL des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten v 5.11.1990, ABl C 1990/277,3.

The reason behind that was that the European Commission did not consider it necessary until 1981 to legislate European rules. [74] A few years later it turned out that just few member states followed the recommendation for an accession to the data protection convention of the Council of Europe, wherefore the commission agreed to create a community legislation. [75] By creation of this data protection directive the European Community took legislative action for the first time in the field of fundamental rights and freedoms. [76] As already said this first draft was preceded by many years of effort pushing for a standardization of the different data protection levels from the European parliament. [77] After the preparation of a second version by the Commission in October 1992, the data protection directive was accepted by the European Parliament and the European Council on October 24, 1995.

3.2.2 Gist of Directive 1995/46/EC

A new era in history of data protection began 1995 with the adoption of the directive whereby two big targets were pursued: [78]

- Article 1 of the DSRL contains on the one hand a clear specification in favor of the priority of free data traffic in the internal market over the hindrance by nation data protection regulations [79].
- On the other hand the DSRL sees itself as an instrument of ascertainment of relevant fundamental rights and fundamental freedoms especially for the protection of privacy by the processing of person related data [80].

3.2.3 Deficits

The data protection directive was enacted before the breakthrough of the internet age. The outdated data protection directive needs to be renewed to guarantee the best available protection of person related data from EU-citizens in the upcoming future.

The fragmentation due to several implementations in the member states and the associated inconsistent jurisdiction of the control instances in the member states, the time consuming registering procedure as well as the complex procedures at border crossing data applications and the problems with the enforcement of rights of affected persons (for example the claim of deletion at Facebook) are fundamental deficits of these particular directive. Due to that the planned and hotly debated data protection regulation is discussed in the chapter *General Data Protection Regulation on page 18.*

[74] Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(92) 422 endg. - SYN287

[75] [Hol02], p.4

[76] [Wes09], p.56

[77] [Hol02], p.4

[78] [Dus09], p.48

[79] Article 1 Section 1 DSRL

[80] Article 1 Section 2 DSRL

3.3 Safe Harbor Agreement

In 2000 the EU and the United States agreed on a "Safe Harbor" procedure for governing the transboundary data transfer [81]. This arrangement enables private enterprises with a residence in the EU to transfer person related data to recipients in the US who are obliged to maintain the European data protection standards. [82] The obligation to observe the agreed "Safe Harbor" procedure is implemented by a Declaration of Compliance or by a certificate of an US-enterprise at the US Department of Commerce. It is also possible to comply via the internet. [83]

The Federal Trade Commission (FTC) is keeping a list [84] with those enterprises which have agreed to comply with the "Safe Harbor" procedure. A data transmission from a European data provider to a certificated US-enterprise is possible without restrictions. [85]

3.4 General Data Protection Regulation

Divergences in the implementation of Directive 95/46/EC led to the prevailing unequal data level in Europe. Currently the 28 member states enact their own laws based on the 1995 Directive. Because of these differences the overall aim of the General Data Protection Regulation is the harmonization of the rules for processing personal data by private companies. The beforementioned regulation is part of the Data Protection Reform which was presented by the European Commission on January 25, 2012. The official title of the General Data Protection Regulation is "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data" [86]. The proposal includes 91 articles on 119 pages. The regulation is intended to replace the national data protection law of all members states, which is based on the Data Protection Directive of 1995 (see *chapter Directive 1995/46/EC on page 16*). Therefore, the General Data Protection Regulation needs not to be transposed into national law. Thus, strengthening or weakening of data protection with separate national regulations is no longer possible. The second part of the Data Protection Reform is a Directive addressed to public authorities, which process relevant data relating to criminal offenses [87].

[81] Commission Decision 2000/520/EC of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce

[82] [Gra10], p.28

[83] [Kny12b], p.120

[84] [Saf]

[85] [Gra10], p.28

[86] [Gen12]

[87] [DRK14]

For better understanding I have illustrated the possible changes in European data protection (see *Figure Structure of data protection laws in the future on page 19*).

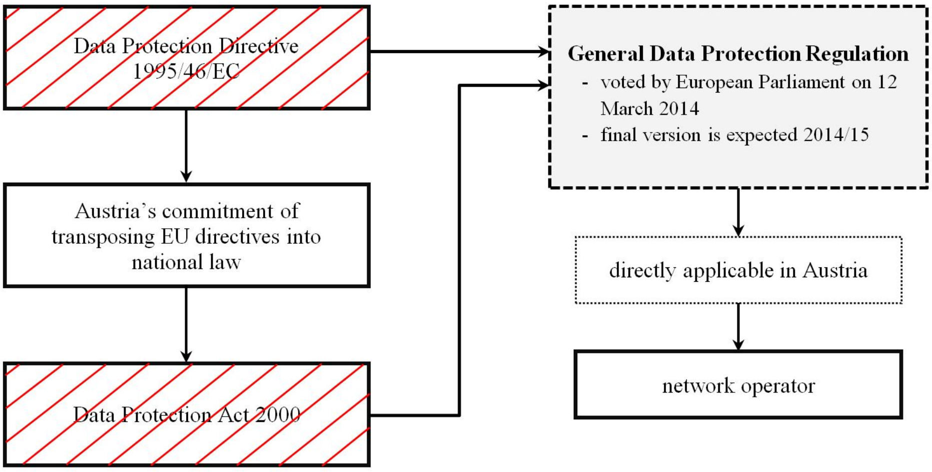
Data Protection Directive 1995/46/EC
Austria`s commitment of transposing EU directives into national law
Data Protection Act 2000
General Data Protection Regulation
- voted by European Parliament on 12 March 2014
- final version is expected 2014/15
directly applicable in Austria
network operator

Figure 3.1: Structure of data protection laws in the future [88]

Companies having its corporate seat outside the EU, but submitting offers to EU citizens, are also concerned. Up to now big American companies, like Google and Facebook, are covered by the Safe Harbor agreement. This would be no longer the case, if the regulation came into effect [89]. Jan Philip Albrecht formulated ten central aspects of the General Data Protection Regulation, which I will discuss in the following paragraph. An essential part is the right of deletion, whereby everyone should have the possibility to request the cancellation of personal data against Google, Facebook & Co. Everyone who illegally publishes data of a person must ensure that each copy is deleted. Moreover, affected persons must be informed about the purpose of data processing and they also must be able to consciously agree to data processing. Another important aspect is a clear formulation of terms and conditions of usage, thus, the usage of standardized symbols instead of too detailed general terms and conditions should simplify either the approval or rejection [90].

Concerning transparency and the obligation to provide information, users should receive comprehensible information on how their personal data are processed or if the provider has transferred data to prosecution authorities or secret services. Another controversial issue raised by a number of member states was the transfer of data to third states. In a former Commission proposal it was determined that data processing by telecommunication and internet companies should be not allowed without explicit consent. Because of intensive lobbying and on behalf of the American government this rule concerning the transfer to third states was deleted. Personal data is that information

[88] [Dr.14]
[89] [Alb13]
[90] [Alb13]

that can be directly or indirectly linked to a person or used to single-out a person from a larger group. Exactly these personal data need to be protected, especially since Big Data becomes more and more important. Up to now most of the companies take penalties into account, but only tough sanctions will discourage companies from considering data protection violations [91]. Another aspect mentioned by Albrecht is concerned with Privacy by Design and Privacy by Default. This means that data processors have to adhere to the principle of data minimization. Based on the principle of data avoidance and data economy, it was also stipulated that there must be the possibility to anonymize or pseudonymize personal data [92]. Furthermore, the appointment of a Data Protection Officer should depend on the amount and relevance of data processing, but not on the size of the company. In order to establish a consistent law enforcement, the European Data Protection Board must ensure the harmonized application of data protection law and should also be able to make decisions, which are now made by national data protection authorities. Therefore, the data protection authorities need more resources and staff to manage the increased workload and they should also be supported by the new European Data Protection Board. The last aspect deals with the "one-stop-shop" approach. Due to this approach citizens should have only one data protection authority throughout the EU to deal with [93].

Rainer Knyrim is an attorney and partner in the law firm Preslmayr Attorneys who discusses relevant Union law and constitutional concerns, a description of the expected effects on Austria and the draft of the concerned regulation in detail. He welcomes the initiative of the European Commission of modernizing the existing Directive 95/46/EC as well as strengthening the individual responsibility of companies. Furthermore, Knyrim is surprised by the scope of the reform proposal, because it conveys the impression that the data protection level in Europe is comparatively low up to now. In fact, Austria and Germany had one of the first data protection acts worldwide and for 30 years a high data protection level [94]. The question is whether the draft regulation complies with the subsidiary principle. According to Article 5 Section 3 TEU, the EU is only able to act within its exclusive competence as long as the objectives of proposed actions cannot be sufficiently achieved either at central or at regional and local level by the member states. The Commission's draft does not sufficiently set out why such a regulation at the European level is required and cannot be achieved by a further development of the previously applicable data protection directive [95].

[91] [Alb13]
[92] [Alb13]
[93] [Alb13]
[94] [Kny12a]
[95] [Kny12a]

3.4.1 Profound changes in the European data protection law

The proposal for a General Data Protection Regulation published by the European Commission on January 25, 2012 provides subsequent profound changes in the European data protection law:

- The national data protection law (DSG 2000) should be replaced by a directly applicable EU regulation in order to establish a standardized EU data protection law. An Austrian characteristic of protecting corporate data by the DSG 2000 would be omitted with the introduction of the EU regulation [96].

- Furthermore, the individual responsibility of companies should be significantly strengthened. Especially the reduction of notification procedures only for specific applications (sensitive data), the internal documentation requirements of companies and the employment of a data protection officer for companies with more than 250 employees should enhance the individual responsibility. In Austria these rules would only apply to 0.3 % of all companies. In contrast to Austrian companies, authorities always must appoint a data protection officer (independently of the size) [97].

- The introduction of an EU-wide "Data Breach Notification Duty" includes the transfer of information to the Data Protection Authority within 24 hours on the one hand and the transfer of information to affected persons with undue delay on the other hand [98].

- Moreover, the imposition of new obligations, for example "Privacy Impact Assessments" for the introduction of new systems, "Privacy by Design" to practice data protection with technology and "Privacy by Default" for making default privacy settings, is also worth mentioning. In addition to the obligations, sector-specific codes of conduct and certifications as well as seals for quality in data protection should be encouraged [99].

- Henceforth, approvals for the utilization of data should only be permitted explicitly, not implied and the client shall bear the burden of proof for the data collection [100].

- Concerned people must be informed about the storage period and the General Data Protection Regulation grants them an extended cancellation right, so called "right to be forgotten". Furthermore, the regulation introduces a "right to data portability" and a right to object to profiling [101].

[96] [Kny12b]
[97] [Kny12b]
[98] [Kny12b]
[99] [Kny12b]
[100] [Kny12b]
[101] [Kny12b]

- The penalties should be increased dramatically in case of violation of requirements laid down in the regulation. In concrete terms this means penalties up to 1 million Euro or two percent of consolidated sales [102].
- The former Austrian provisions on a joint information system will be implemented in the regulation as well in a way that joint controllers share responsibility and are jointly and severally liable for the entire damage. Besides that, controllers and service providers should continue to be jointly and severally liable, which requires a redesign of service agreements [103].
- In order to facilitate the cooperation between corporations and authorities, the regulation is obliged to introduce a so called "one-stop-shop". According to this approach the data protection authority at the headquarter is responsible for the supervision of its processing capacity in all Member States [104].
- Principles of international data transfer beyond the borders of the EU will be on the one hand maintained (standard contractual clauses and equivalent countries) and on the other hand extended (model for binding corporate rules, so called "Binding Corporate Rules") [105].

3.4.2 Comparison between current and future regulative

Currently the EU Data Protection Directive of 1995 was implemented by national data protection laws, whereas the competent control authorities are the national data protection authorities [106].

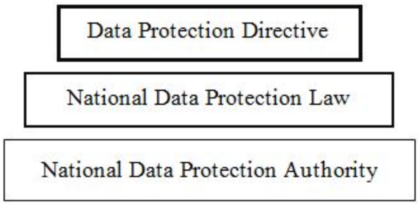
Data Protection Directive
National Data Protection Law
National Data Protection Authority

Figure 3.2: Current architecture of data protection in the European Union [107]

[102] [Kny12b]
[103] [Kny12b]
[104] [Kny12b]
[105] [Kny12b]
[106] [Kny12a]
[107] [Kny12a]

In accordance with the current proposal, the concerned Directive and the National Data Protection Act will be replaced by a regulation with direct application and replacing numerous implementing regulations of the member states. The Commission may suspend decisions of the national data protection authorities, although foreign data protection authorities can act against the national data protection authority [108].

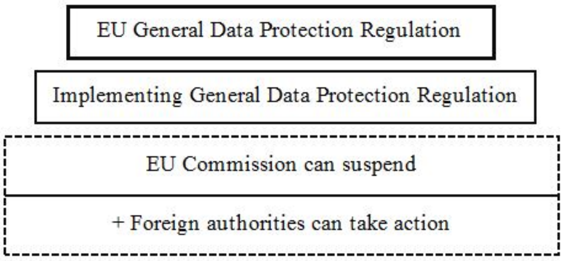
EU General Data Protection Regulation
Implementing General Data Protection Regulation
EU Commission can suspend
+ Foreign authorities can take action

Figure 3.3: Architecture with implementation of General Data Protection Regulation [109]

3.5 Directive 2002/58/EC and Directive 2009/136/EC

The Directive 2002/58/EC was part of the "Telecoms Package", a new legislative framework designed to regulate the electronic communications sector and replace the existing regulations governing the telecommunications sector. Generally speaking, this Directive concerns the processing of personal data relating to the delivery of communication services [110].

The Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) has been modified twice since its entry into force, namely in 2006 [111] and in 2009 [112]. The latest amendment of Directive 2002/58/EC was made by Article 2 of Directive 2009/136/EC on December 19, 2009. The Directive 2009/136/EC is also known as "Cookie Directive" or "e-Privacy Directive" and had to be transposed into national law until May 25, 2011. The primary target group of this directive is the advertising industry, which uses cookies for creation of user profiles. Before moving on to the central points of the Cookie Directive, I want to explain the concept of cookies. A cookie is a small file including user-specific data that is installed on a computer of a user when visiting a website by the server itself.

[108] [Kny12a]
[109] [Kny12a]
[110] [Com10]
[111] Directive 2006/24/EC
[112] Directive 2009/136/EC

Because of the information contained therein, once entered data such as password on a website, can be automatically generated again as well as offering special products in online shops becomes possible. Cookies, however, can also track the users surfing behavior. The e-Privacy Directive determines that the use of cookies, which serves not only the sole purpose of carrying out the transmission of a communication over an electronic communications network or an information society service explicitly requested by the subscriber or user, is only allowed with the user's consent[113]. A further prerequisite is the provision of comprehensive information on the user on the use of cookie technologies as well as referring to the generated data. Setting a cookie in the context of an online store for the assignment of the shopping cart to a user is still possible without consent, whereas the use of cookies for the evaluation of the user's browsing habits is not possible without the assent of those involved. The transposition of the Directive 2009/136/EC into national law might pose some problems; especially the ambiguous wording of Article 5 (3) of the directive offers a high degree of flexibility in implementation. The active consent of a user in respect of the use of cookies is referred to as "opt-in", whereas "opt-out" offers the user the possibility to object to the use of cookies. The EU Members States have taken advantage of this leeway and implemented Article 5 (3) of the directive differently. Finland and Portugal had already implemented the opt-out solution while the majority decided to use opt-in. Some national transposing laws stick rigidly to the text of the present e-Privacy Directive, which leads to legal uncertainty. It remains to consider that the legal situation in Europe varies widely from country to country. European companies based outside the European Economic Area have difficulties with the existing regulations, because of different national requirements for one and the same website. [114] [115]

3.6 Directive 2006/24/EC

The European Union's Data Retention Directive 2006/24/EC [116] was introduced due to the terrorist attacks in Madrid of March 11, 2004 and London of July 7, 2005. Moreover, the different data retention approaches on national levels resulted in lack of a competency in criminal law, which could be overcome with the establishment of a harmonized framework on EU level. Data Retention requires providers of telecommunication, mobile and internet services to save and retain the traffic and location data of users. All personal data is extensively stored without initial suspicion or concrete warnings of hazards. The key factor behind the development of the directive were the terrorist attacks in London, Madrid and New York. [117] The European Union reacted to these terrorist attacks and enacted the Directive 2006/24/EC, whereas this data retention directive is since its creation legally controversial. [118]

[113] Article 5 (3) of Directive 2009/136/EC

[114] [RA 12], p.16

[115] [RA 14], p.68

[116] [Dir06]

[117] [Jas10]

[118] [Lud08]

3.6.1 Historical development

The police and afterwords also the political decisionmakers of several members states of the European Union strongly urged the introduction of such a monitoring tool to effectively combat terrorism and serious crime. Even before the terrorist attacks of 9/11 happened, a discussion about the storage of telecommunication data arose in Spring 2001. At that time the British civil rights organization "Statewatch" reported of a European police working group's demands of storing communication data, emails and website accesses for at least seven years [119]. A few days after the terrorist attacks in the United States, the Council of Justice and Home Affairs had requested the European Commission to develop a proposal to enable security agencies to successfully detect and investigate criminal activities (when using electronic telecommunications opportunities). The Council stated that the balance between the protection of personal data and the needs of law enforcement agencies remains protected [120].

A year later on December 19, 2002 the Council of Justice and Home Affairs emphasized in its conclusions that the personal data generated by the increasing use of electronic telecommunications possibilities had become an important tool for investigating criminal offenses, especially organized crime [121]. In 2002, Denmark had the presidency of the EU Council. In a first draft of the Directive the duration of storage was limited to twelve months, but this draft was rejected by a majority. Amongst other things, the terrorist attacks in the Spanish capital Madrid prompted the European Council commissioning the Council of Ministers to consider which legal provisions were required for data retention. Another reason for the introduction of this Directive was the rising international crime rate. The framework decision of April 28, 2004, submitted by France, Ireland, Sweden and the United Kingdom, provides for a minimum storage of 12 months and a maximum storage of 36 months [122]. This framework decision should not only help in preventing crime, but also in investigating and prosecuting crimes, which have already been committed. Various critics and opponents of data retention had requested an EU Directive, because the framework decision of the Council was insufficient in their eyes.

Aside of the development of the Directive the Council was still working on the framework decision till 2005. Unfortunately, unanimity in the Council of Ministers could not be reached, because the different governments were not able to agree on the storage period [123]. In 2005 terrorist attacks occurred in London and the United Kingdom took over the Council's Presidency. Thus, the project of introducing a Data Retention Directive gained new momentum. The EU commission developed a new draft in September 2005, which should represent a good compromise between the different interests of data retention proponents and opponents. According to this draft, internet data should be stored for six months and traditional telephony data for at least 12 months. The European Parliament amended the commission's draft insofar as the Directive should

[119] [LS14]
[120] [oJA01]
[121] [oJA02]
[122] [Rat04]
[123] [fM09a]

only be used for the prosecution of serious criminal offenses. [124]

Furthermore, the catalog of data types that must be stored compulsory was shortened and the balance between freedom and safety was paramount within this modified draft. The before mentioned draft was also called "Alvaro draft" and was again rejected by the proponents and opponents. The Council of Ministers negotiated again and created the so called compromise proposal, wherein a margin of six to 24 months is permitted for the storage period. [125] On December 14, 2005 the European Parliament had successfully voted on the compromise proposal and despite long negotiations and repeated changes the Directive was adopted after only three months as the "fastest Directive" of the EU. In February 2006 the Council of Ministers agreed by a majority; only Denmark and Slovakia voted against the Directive because of formal reasons. Notwithstanding the proposal from the European Commission, however, retention periods for all communication data of not less than six months and not more than two years are prescribed in the Directive as adopted by the Council. The Data Retention Directive had been adopted on March 15, 2006 and had to be transposed into national law by September 15, 2007. Austria made a declaration that the storage of internet data could be suspended until March 2009. [126]

3.6.2 Structure and details of the Directive

The Data Retention Directive is more precisely known as the Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. The Directive was adopted by the European Parliament and the Council of the European Union based on a proposal of the Commission and consists of 17 articles. According to Article 4 the member states must take appropriate measures to ensure that the retained data shall be transmitted only in specific cases and in accordance with the national law of the competent authority, whereas Article 15 determines the deadline for transposition into national law [127]. The Directive 2006/24/EC refers to two other EU Directives. First, the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and second the Directive on privacy and electronic communications supplement the Data Retention Directive [128].

[124] [fM09a]
[125] [fM09a]
[126] [fM09b]
[127] [Dir06]
[128] [fM09b]

3.6.3 Current legal situation

On April 8, 2014 the Court of Justice of the European Union, shortly ECJ, has invalidated the EU Directive 2006/24/EC on the retention of telecommunication data on stock from the date of its entry into force [129]. Subsequently, the Austrian Constitutional Court has Austrian laws on Data Retention found unconstitutional, because the legal provisions are in contradiction with data protection and the right to privacy. As stated in a press release [130] of the Constitutional Court the Austrian laws "contradict the fundamental right to data protection and Article 8 of the European Convention on Human Rights." [131] Moreover a "deadline for rectification is not granted" and the "repeal takes effect upon its promulgation, which shall be made immediately by the Federal Chancellor." [132]

[129] [Cou14]

[130] [N.N14d]

[131] Article 8 – Right to respect for private and family life [N.Na]

1) Everyone has the right to respect for his private and family life, his home and his correspondence.

2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[132] [N.N14b], G 47/2012

3.7 OECD Guidelines

The OECD is an international organization based in Paris, France, with 34 member states from all over the world. [133] The convention establishing the organization of economic cooperation and development, consisting of 21 articles, was signed on December 14, 1960 by the following countries: Belgium, Denmark, Greece, Ireland, Germany, France, Iceland, Italy, Canada, Luxembourg, Netherlands, Norway, Austria, Portugal, Sweden, Switzerland, Spain, Turkey, Great Britain, Northern Ireland and the USA. [134]

The OECD detected the need for an international arrangement on data protection and on September 23, 1980 passed guidelines for the protection of privacy and the border crossing transfer of person related data. [135] These guidelines are based on the three principles "respect of human rights", "free market economy" and "pluralist democracy" which the OECD member states are committed to. [136]

Furthermore, these guidelines contain material and procedural arrangements for the public and the private sector but are, however, not binding international law. The member states are free to transform these guidelines into national data law; nevertheless far more states joined this document than committed by the EU regulation. The articles 7 [137], 8 [138], 9 [139] and 10 [140] are defining the essence of the principles of use of data like in the privacy policy respectively in the data protection law of DSG 2000 where these principles are already implemented. [141]

[133] [Bun]

[134] [OEC60]

[135] [COD03], p.2

[136] OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980), Document C (80) 58 (Final), Bekanntgabe Banz, Amtl. Teil v. 14.11.1981, Nr. 215; s. a. OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007).

[137] **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. [Ger09]

[138] **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. [Ger09]

[139] **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. [Ger09]

[140] **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law. [Ger09]

[141] [Lec09], p.212

CHAPTER 4

Privacy issues in America

The digitalization by increased cross-linking of customers and spectacular cases of data abuse let the consciousness for data protection in the USA grow. Data protection is already a very current topic in the USA, however, the comparison between the European data protection law and the American legislation relevant for data protection is very difficult. There is no encompassing and comparable data protection law in the USA like there is in Europe, it would perhaps be described as data protection landscape. The Federal Trade Commission is an independent federal authority of the USA and is among other things responsible for consumer protection. The FTC does not certificate enterprises and contrary to the European data protection authority it just takes action if consumer, enterprises or politicians lodge a complaint. [142]

According to a ruling of the Commission of the European Communities of July 26, 2000 over the appropriateness of the guaranteed protection by the principles of the "Safe Harbor" the USA uses in terms of the data protection law, "a sectoral approach, which is based on a mixture of legal regulations, directives and self-regulation." [143]

The USA distinguishes in data protection between Privacy Acts and Privacy Protection Acts.[144]

The data protection legislative includes among other regulations the following acts

- the Electronic Communication Privacy Act, [145]
- the Privacy Act, [146]

[142] [Aig11]

[143] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)

[144] [Mül10], p.93

[145] [Mül08], p.106

[146] [Mül08], p.106

- the Gramm-Leach-Bliley Act (GLBA) with the implementations of the Federal Trade Commission in the "Standards for Safeguarding Customer Information", 16 CFR 314 [147]

- the Social Security Act, [148]

- the Driver's Privacy Protection Act (DPPA) [149]

- the Financial Services Modernization Act of 1999 [150]

- the Family Educational Rights and Privacy Act (FERPA) [151] and the

- Children's Online Privacy Protection Act. [152]

Referring to the real cases in *chapter "Real-life examples of losing control"*, I am going to discuss the Children's Online Privacy Protection Act in the following part more precisely.

4.1 Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act, briefly COPPA [153], regulates the protection of person related data of children under the age of 13 in the online sector since the 21th of October 1998 [154]. Passed by the U.S. Congress in 1998, the law took effect in April 2000. COPPA is not just relevant for commercial websites and online services, but also for apps and online video games, which are addressed to children under the age of 13 and collect, utilize and transmit this particular person related data.

To protect children, the Act imposes requirements on operators of websites or online services directed to children under the age of 13 as well as other operators with actual knowledge that they have collected personal information from children. [155]

The legal guardians obtain the opportunity to decide over the collection and processing of their children's data via a prior consent. [156] This parent's approval has to be submitted before starting data processing. [157]

[147] cf. http://www.law.cornell.edu/cfr/text/16/part-314
[148] [Mül08], p.106
[149] [Mül10], p.93-94
[150] [Mül10], p.93-94
[151] [Mül10], p.93-94
[152] 15 U.S.C. §§6501-6508 (2001).
[153] COPPA must not be confused with the defunct Child Online Protection Act (COPA)
[154] [Gen04b], p.68
[155] [Hil14]
[156] 15 U.S.C.A. Sec. 1302
[157] 15 U.S.C.A. Sec. 1303

COPPA induced huge international impact, so that even (commercial) websites which are not either under US jurisdiction, or whose servers or headquarters are not located in the US, started blocking children under the age of 13. [158] [159]

As already mentioned, COPPA is also relevant in Austria, if (1) websites, video games or apps are addressed to children in the USA, but also (2) if personal data of US American children under the age of 13 is captured and processed.

As the Article "Guide to Compliance with the Amended COPPA Rule" of Cynthia Larose and Julia Siripurapu [160] illustrates, the requirements which COPPA extends to operators and developers comply substantially to the basic statements of European data protection law. [161] The amended COPPA Rule was issued by the FTC on December 12, 2012, with an effective date of July 1, 2013 [162], whereas operators are now obliged to:

- "Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from persons under the age of 13;
- Make reasonable efforts (taking into account available technology) to provide direct notice to parents of the operator's practices with regard to the collection, use, or disclosure of personal information from persons under 13, including notice of any material change to such practices to which the parents has previously consented;
- Obtain verifiable parental consent, with limited exceptions, prior to any collection, use, and/or disclosure of personal information from persons under the age of 13;
- Provide a reasonable means for a parent to review the personal information collected from their child and to refuse to permit its further use or maintenance;
- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected from children under the age of 13, including by taking reasonable steps to disclose/release such personal information only to parties capable of maintaining its confidentiality and security; and
- retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.
- Operators are prohibited from conditioning a child's participation in an online activity on the child providing more information than is reasonably necessary to participate in that activity." [163]

[158] [Com07]

[159] cf. COPPA Rule's definition of an "operator", which includes foreign websites that are involved in commerce in the United States or its territories. FTC Final Rule, Children's Online Privacy Protection Rule, 16 C.F.R. Part 312

[160] [CJL13]

[161] [Hil14]

[162] [Mat14b]

[163] [CJL13], Section: What Must Operators Covered by the Rule Do to Comply with COPPA?

Violations of COPPA will be punished by a fine of up to 16.000 USD. In the development of Apps, video games or other online services it is recommended to familiarize with both the European law and the American law in form of COPPA to avoid the threatened fines. [164]

[164] [Hil14]

CHAPTER 5

Austrian law

5.1 Data Protection Generations

Currently, there exists the Data Protection Act 2000 in the fourth generation. To understand the intention of this act I want to start 30 years ago because nowadays we distinguish between four generations of data protection. The first generation of data protection resulted from the intention of the state as well as companies to store the data in central and national databases. The risk of adverse data usage had been compared with the dangers of producing nuclear energy. Consequently, this risk had to be reduced. The original concept of central databases had not been implemented to the full extent when information technology developed in quite a different direction. Instead of centrality the use of cheaper and more efficient computers became more and more popular within the second generation of data protection. With this development the risk of adverse data usage is not restricted solely to a few central databases but is distributed to a myriad of systems. People who were affected by the distributed storage of their personal data started to claim the rights on their data from the parties responsible. Therefore, the data protection act 1978 included rights of concerned parties emphasized on privacy protection and sustained slowdown in IT norms [165]. The third generation was characterized by informational self-determination which was in the following years the fundamental basis for the development of European data protection legislation. However, informational self-determination did not automatically give the citizens the opportunity to claim their rights. In certain sectors (for instance in telecommunications or direct marketing) special problems in data protection arose which could not be solved with general data protection legislation. Due to this fact the data protection standards were extended with a special focus and emphasis on rights of affected people, improving liability by a reversal of the burden of proof, fault regulations and sectoral regulations (data protection legislation for electronic communication) in the fourth generation [166]. The European fundamental right

[165] [Vik14]

[166] [Dir02]

of data protection (Article 8 European Charter of Fundamental Rights [167]) is anchored in the Treaty of Lisbon [168]. Article 8 of the European Charter of Fundamental Rights is an effective tool for securing the rights of affected people. On the 25th of January 2012 the European Commission has submitted a proposal for a basic regulation on data protection which would change the basis of European data protection fundamentally in many areas [169] [170]. The first reading in the European Parliament has taken place in March 2014. The further progress of the legislative process at the European level remains to be seen. From my personal point of view I think that the fifth generation is soon to be awaited.

5.2 Data Protection Act 2000

Austria's first Data Protection Act of October 18, 1978 [171] was based on a government bill of 1975 and came into force on January 1, 1980. Paragraph 1 of this first Data Protection Act (DSG) already included the fundamental right to privacy, but strictly separated the private and the public sector. The DSG has been amended several times and it was originally planned to implement the European Data Protection Directive by a further amendment to the DSG. [172]. While preparing this amendment, the wish for abandoning the division of DSG into a public and a private sector was frequently expressed. This desire could only be realized with the introduction of a completely new Data Protection Act 2000, although at least in respect of completed authorities the duality was essentially maintained (Data Protection Commission in the public sector and civil courts in the private sector) [173]. On January 1, 2000 the Austrian Data Protection Act 2000 [174] entered into force and has replaced the previous Data Protection Act of 1978 [175]. This new and current Data Protection Act 2000 attempts to maintain already proven control structures of the old DSG [176].

The Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector is implemented in the Telecommunications Act 2003 (TKG 2003) [177] and regulates contents related to the Internet, including cookies, log files and the interception of telephone communications. More details about the directive on privacy and electronic communications are explained in detail in *chapter Directive 2002/58/EC and Directive 2009/136/EC on page 23.* To comply with the technical developments, a ministerial draft for the amendment of the DSG was presented in 2008

[167] [Cha00]
[168] [Tre07]
[169] [SK13]
[170] [Gen12]
[171] [DSG78]
[172] [Dir95]
[173] [Kny12b]
[174] [DSG14]
[175] [DSG78]
[176] [Kny12b]
[177] [Dir02]

[178]. There were plans for simplification of the formulation of fundamental rights, for a sole jurisdiction of the Federation to terminate the fragmentation in federal and state privacy laws, introduction of a data protection officer and the regulation of video surveillance by private persons. Due to the political situation and the then dissolution of the Austrian Parliament this amendment was never adopted. However, the amendment of the DSG was tackled again in June 2009 [179]. An agreement regarding the proposed simplification of the constitutional provision and the clarification of competences could not be achieved because of a lack of political majority for constitutional amendments [180].

5.2.1 Fundamental Right to Data Protection

The Data Protection Act 2000 consists, as well as the DSG 1978, of two separate articles. Article 1 includes Section 1, which defines the fundamental right to privacy, whereas Article 2 contains all other provisions on data protection. Moreover, the fundamental right to data protection arises from the right for respect of private and family life, which is defined in Article 8 of the European Convention on Human Rights [181]. The fundamental right to data protection is defined as follows:

> §1. (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to data subject's intend in secrecy due to their general availability or because they cannot be traced back to the data subject.

[178] [Bun08]

[179] [Bun09]

[180] [Kny12b]

[181] [Kny12b]

5.2.2 Three actors in the Data Protection Act

The Data Protection Act distinguishes between three actors, namely, a controller, a processor and a data subject. As evident in the *figure Correlation of three actors*, the data transmission requires the definition of a fourth actor. In contrast to the before mentioned actors, the data recipient is an outsider and is often called third party [182].

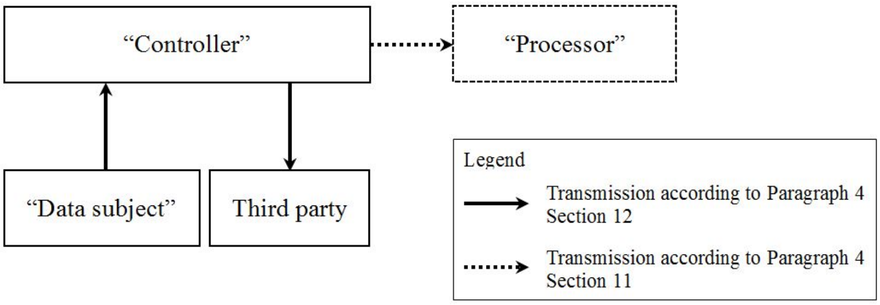
"Controller"
"Processor"
"Data subject"
Third party
Legend
Transmission according to Paragraph 4 Section 12
Transmission according to Paragraph 4 Section 11

Figure 5.1: Correlation of three actors [183]

5.2.2.1 Data subject

Data subject is a frequently used term in data protection law and is defined as any natural or legal person or group of persons, whose data are processed (Article 2 Paragraph 4 Section 3 DSG) [184].

5.2.2.2 Controller

A controller is in accordance with Paragraph 4 Section 4 DSG

- a natural or legal person, associations of persons or bodies of a local authority or the offices of these institutions,
- if they decide alone or jointly with others about the use of personal data (Section 8)
- without regard whether they use the data by themselves (Section 8) or commissioning on processors (Section 5).
- They are also considered as controllers, if the authorized processors (Section 5) use personal data for producing a work (Section 8), unless the service provider is prohibited from the usage or the contractor has to decide autonomously on the basis of rules of law or codes of conduct.

[182] [Kny12b]
[183] [Kny12b]
[184] [Kny12b]

Therefore controllers may be either natural persons or companies. For the definition of the controller it is decisive that the controller alone or with others decides to process data. Perhaps I can mention a few examples for clarifying this definition:

- Firstly, a doctor who stores personal data of his patients is the controller of the patient data management.

- Secondly, a retail merchant who stores data of its customers is also client of the customer data management.

- As the final example I want to mention that companies processing personal information of employees for accounting are, however, controllers of personnel data management.

In contrast to the processor, the controller still owns the data and is responsible for

- maintaining the quality principles (§ 6 DSG 2000),

- the verification of admissibility conditions (§ 7 DSG 2000),

- compliance with the legitimate confidentiality interests (§§ 8 and 9 DSG 2000),

- the examination of criteria for the acceptable use of an experienced processor (§§ 10 and 11 DSG 2000),

- the application for an approval for a transfer, which is subject to approval and surrendering data to foreign countries (§ 13 DSG 2000) and many more.

5.2.2.3 Processor

Processors are, pursuent to Article 2 Paragraph 4 Section 5 DSG, natural or legal persons, a group of persons or an organ of a federal, state and local authority or rather the offices of these organs, whereas they use the data only for the production of a commissioned work (Section 9) [185].

The demarcation between a controller and a processor is cautious: If the processor explicitly prohibits data processing on the occasion of placing an order or makes his own autonomous decisions concerning the way of using personal data, the processor itself is considered as a data protection controller. Generally speaking, the distinction between controller and processor is particularly difficult in larger companies or groups in which departments provide services to other departments.

[185] [Kny12b]

5.2.3 Application scope of DSG 2000

5.2.3.1 Material scope

The DSG 2000 covers the protection of personal data of everybody, in detail data from natural and legal persons [186], groups of persons [187] and also automatically processed and manually processed data. The previous version of the data protection act contained only automatically processed data, but the scope of the DSG 2000 has been extended and includes now manually processed data. As for the data subject, [188] not only a natural person can be affected but also legal persons and associations. [189] This additional protection of enterprise data is guaranteed in just a few member states of the EU, apart from Austria in Denmark, Luxembourg and Italy. Due to this definition, B2C enterprises and also B2B enterprises are covered by law. In terms of manually processed data there is a restriction, since these data is only covered by law if it is saved to a file which is a structured set of data with an own search criterion. [190] Possible examples for that are lists or card indexes structured by one or more search criterions. [191]

5.2.3.2 Territorial scope

The territorial scope extends over all data usage which occurs within the domestic territory. [192] Everyone (domestic or foreign persons, but also enterprises) who is running a data application is covered by the Austrian data protection act. The residence principle has an only exceptional character and it focuses on the headquarters and subsidiaries of the enterprises: Data Protection Act 2000 is applicable for data applications in other EU member states, when these data applications are subject of Austrian company's headquarter or branch. [193]

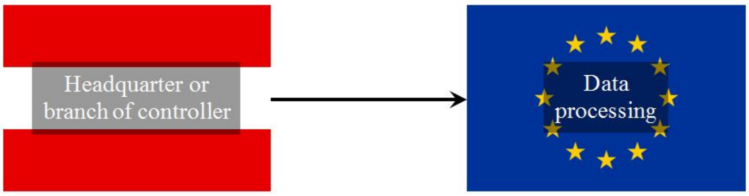

Figure 5.2: Data usage for the purpose of domestically located headquarters or branch - application of the Austrian data protection law [194]

[186] GmbH and AG
[187] GesbR, ARGE, OG
[188] § 4 Section (3) DSG 2000
[189] [Kny12b], p.11-12
[190] § 4 Section (6) DSG 2000
[191] [Kny12b], p.12-13
[192] § 3 Section 1 (1) DSG 2000
[193] § 3 Section 1 (2) DSG 2000
[194] [Gra10], p.33

Vice versa the law of another member state has to be applied in Austria if there is a private controller with headquarter in another member state of the EU who uses data in Austria without maintaining a permanent establishment there. [195] A subsidiary is clearly defined in § 4 Section 15 DSG 2000 and characterized by a territorial and functional limited organizational unit (with or without legal personality) which is operating at the location of their facility. [196]

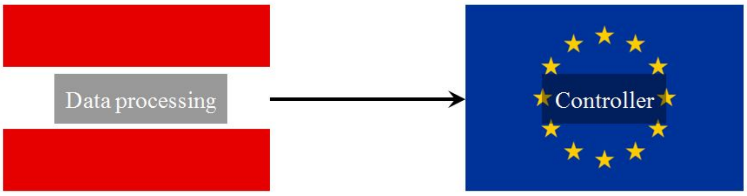

Figure 5.3: Processing in Austria for purposes that are not ascribed to any domestic branch - application of the law of member state, in which the (private) controllers headquarter is located [197]

To put it briefly, a subsidiary within the meaning of DSG only exists if the processed data is also in a tangible connection with the subsidiary. In contrary a processing of tangible strange data is not covered by the local law [198]. There are two examples given to define more clearly these theoretical explanations:

- The representative of an Austrian beer supplier sells beer in Germany and processes German customer and order data on his notebook. This customer and order data administration is covered by the Austrian data protection act. [199]

- A German mail-order house collects by German marketing personnel data of interested parties for use of catalogues in an Austrian subsidiary. This data processing is admittedly covered by the German Bundesdatenschutzgesetz. [200]

The simple transmission of data like the transmission over the internet via switches and wires in Austria, where the start and end point is abroad, is not covered by Austrian law. In this case the law of the sending or receiving country is crucial. [201]

[195] § 3 Section 2 DSG 2000
[196] [Kny12b], p.13
[197] [Gra10], p.33
[198] [Son10], p.244
[199] [Kny12b], p.13
[200] [Kny12b], p.13
[201] [Son10], p.245

5.3 Rights of affected persons

5.3.1 Duty of employer to provide information

This obligation to provide information [202] defines that the controller has to inform the data subjects on the occasion of the investigation of data by providing the purpose of the application as well as the name and the address of the controller even if those data subjects did not make an application in that case. [203] This duty of providing information should ease the problem to enforce the rights of the affected persons (right to information, right of rectification and solution and the right of opposition); admittedly the verbalization of the paragraph is very short and leaves room for interpretation. [204]

The data protection directive of the EU has committed the Austrian legislator to implement a proactive duty of information. That means that the purchaser has to inform the concerned person immediately at the beginning of the data obtaining. [205] [206]

In the following cases, for example, there exists no duty to provide information [207]:

1. The information is already available for people concerned. [208]
2. There is only indirectly person related data processed. [209]
3. Data is processed within the scope of standard applications or is used for journalistic aims. [210] [211]
4. Data applications are exclusively used for personal or familiar activities. [212]

For several years there has been in the US a "Data Breach Notification Duty". With the Data Protection Act 2000 amendment, the Austrian data breach notification has been implemented: [213]

> §24 (2a) DSG 2000: If the controller learns that data from his data application are systematically and seriously misused and the data subject may suffer damages, he shall immediately inform the data subject in appropriate manner. Such obligation does not exist if the information - taking into consideration that only minor damage to the data subject is likely and the cost of the information to all persons concerned - would require an inappropriate effort.

[202] § 24 (1) DSG 2000

[203] [Gra10], p.68

[204] [Vik14], p.38

[205] [Vik14], p.36

[206] The omission must be remedied without delay, if the information of the person concerned was not possible when recording the investigation.

[207] § 17 Section 2 and 3 DSG 2000

[208] § 17 Section 2 Clause 1 and 2

[209] § 17 Section 2 Clause 3

[210] [Vik14], p.36-37

[211] § 17 Section 2 Clause 4 and 5

[212] § 17 Section 2 Clause 4 and 5

[213] [Rai10], p.297, [Kny10], p.59, [Mar13]

5.3.2 Obligation to disclose the identity of the controller

The controller has to disclose his identity [214] in a suitable manner by transmission and notification so that the concerned party has the opportunity to assert their rights. [215] By the use of standard applications the purchaser is committed to ensure the transparency and he/she has to inform everyone on request which standard applications are actually performed. [216] The registration number of the controller has to be transmitted to the data subject if data applications are used which are subject to registration. The legislator ensures that detailed information concerning the identity of the controller is available. [217] By exercising the control tasks, data applications which are not subject to registration have to be revealed to the data protection authority.

5.3.3 Right of access to data

Everyone has in accordance to legal requirements the right to [218]

1. the processed data
2. available information about the data origin
3. the purpose of data processing
4. possible recipients of transmission
5. as well as legal foundations. [219]

The data subject has to hand in a written request of information and also has to prove its identity but there is the possibility to make this request orally with the approval of the controller. The crucial part is the proof of identity, because this is the precondition for the crystallization of the entitlement of information and the eight week time limit for replying to the information request starts by the submission of the proof of identity. If the information is not transmitted, there has to follow a justification within eight weeks. [220] The right of access to data does not grant the right of inspection of files. [221] At the insertion of the information request it is recommended to use a template letter because the reply may occur quicker (see *figure Information enquiry procedure*).

[214] § 23 DSG 2000 and § 24 (1) Clause 2
[215] [Vik14], p.37
[216] [Gra10], p.68
[217] [Vik14], p.37
[218] § 26 DSG 2000
[219] [Kny12b], p. 276
[220] [Vik14], p.38
[221] VwGH 28.01.2014, 2003/12/0173
[222] [Kny12b], p.278

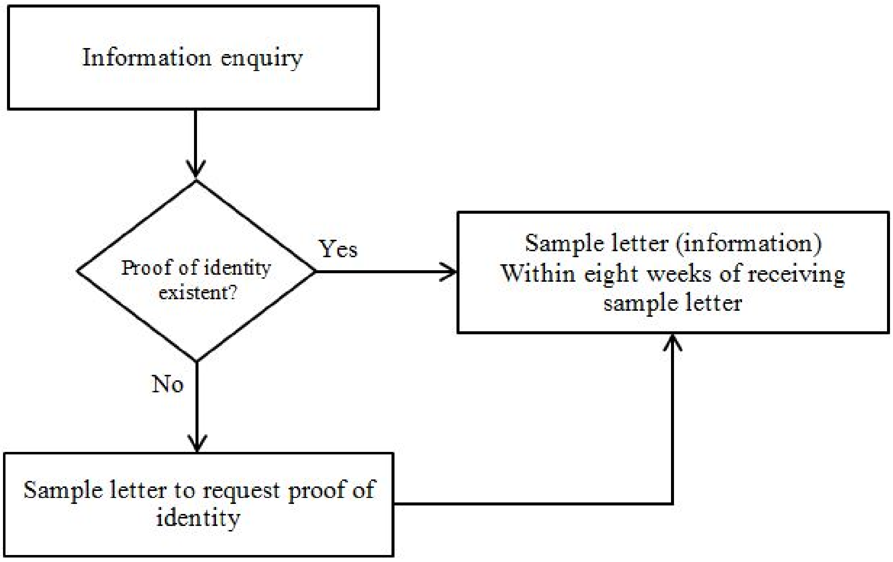
Information enquiry
Proof of identity existent?
Yes
No
Sample letter (information) Within eight weeks of receiving sample letter
Sample letter to request proof of identity

Figure 5.4: Information enquiry procedure [222]

Basically the exchange of information is free of charge if it (1) relates to the current data stock/pool and (2) the data subject has not submitted a request for information in the same remit.

5.3.4 Right of rectification and cancellation [223]

Originally the right of rectification and deletion in the DSG 1978 [224] was considered separately; however, those topics were consolidated in the DSG amendment of 2010. [225] Every controller has the obligation to rectify or delete incorrect or illegally processed data as soon as the incorrectness of data or the inadmissibility of use became known. [226] The DSG amendment of 2010 brought another significant innovation because the rectification or deletion is excluded as far as the purpose of documentation relating to a data application does not allow subsequent changes. [227] The obligation of rectification affects just data where the correctness is relevant for the purpose of data application. § 27 Section 1 DSG 2000 determines, that data which is no longer necessary for the purpose of data application, is classified as inadmissible and this data has to be deleted immediately. The Supreme Court has noted that "delete" within the meaning of DSG 2000 means a "physical" and not a mere "logical" deletion of data. [228]

[223] § 27 DSG 2000
[224] §§ 12, 16 and 27 DSG 1978
[225] [Vik14], p.40
[226] [Gra10], p.71
[227] § 27 Section 3 DSG 2000
[228] [Son10], p.280

5.3.5 Right to object

Besides the right of information, rectification or deletion, data subjects have also the right to protest against the processor regards the usage of their data due to a violation of protected secrecy interests resulting from their particular situation. [229] This right exists only if (1) the usage of data is not intended by law and (2) the protected secrecy interests are violated resulting from the particular situation of the data subject. [230] The exercise of the right to object [231] has no influence on the legal admissibility of the data application, but causes an individual obligation of deletion which is restricted to those affected. [232] The processor has the duty to delete the data of the affected ones on their request within 8 weeks and he also has to ensure that there is no more transmission of this particular data. [233] [234] In contrast to cases involving the right of deletion the data is processed correctly and lawfully though data subjects are able to prohibit the usage of their data due to special circumstances which have to be justified concretely. [235] At the DSG amendment 2010 there were also some adjustments [236] at the topic "right to object" whereupon for example some regulations regarding the right of rectification and deletion [237] also apply to the right of objection.

[229] § 28 Section 1 DSG 2000

[230] [Kny12b], p.281

[231] § 28 DSG 2000

[232] [Gra10], p.72

[233] [Vik14], p.41

[234] [Son10], p.243

[235] [Son10], p.243

[236] § 28 Section 3 DSG 2000

[237] § 27 Section 4, 5 and 6 DSG 2000

CHAPTER 6

Loss of control

6.1 Hot topics

This chapter starts with a collection of hot topics that deliberately show less well-known examples of loss of control. Regardless of whether posting a photo on Facebook or storing data in a cloud - sharing means a loss of control.

6.1.1 Pleaserobme.com

The Web 2.0 platform "Pleaserobme.com" was launched by three Dutch persons, namely Barry Borsboom, Frank Groenveld and Boy van Amstel [238], to raise awareness about online privacy issues, especially locational privacy and social networking behaviour. Those three members work for a concept and idea factory called Forthehack. [239] Pleaserobme.com provides real-time updates on empty homes using Twitter and Foursquare to show all the connections and opportunities of networking for this particular information. Obviously this platform was not built as a service for thieves and robbers, it was just developed as a warning and reminder for users of social networks not to disclose too much data. [240] Pleaserobme.com went online on February 17, 2010, but was taken down shortly after the launch. [241] For the sake of completeness I want to give some background information: Twitter is a real-time microblogging application. Registered users create short text messages, so called tweets, which other users can follow. One of the most spectacular tweets in the history of Twitter is the eyewitness account of Janis Krum of the aircraft emergency landing in the Hudson River on January 15, 2009:

[238] [Kar13]

[239] [N.N09]

[240] [Pat10]

[241] [Kar13]

"There's a plane in the Hudson. I'm on the ferry going to pick up the people. Crazy." [242]

Foursquare is an increasingly popular location-based social network, however, mainly performed for smartphones. Users "check in" to a location and share this information with friends using this service too. [243] This platform should also call attention to some personal information which is posted willingly by persons who are not able to realize the consequences of a possible misuse. If these two per se irrelevant data flows of Foursquare and Twitter are joined, even more personal information results from this operation as originally was put on the two separate platforms. The extreme attention which was caught up by this humorous websites is still presented in an audio visual presentation. The headlines on the front pages of numerous online magazines that are going around the world have encouraged the Dutch founders of this website in their project. Forthehack is "satisfied with the attention they have gotten for an issue they deeply care about" and promise that "as soon as they find a suitable way to continue", they will. [244] The message of Forthehack which should have been conveyed – "Be aware, what you share!" – has taken a fascinating development by this simple platform. The effort of the creation of Pleaserobme.com is vanishingly small: Half a day of brainstorming, four hours for designing and programming and occasionally some pizza. [245] In this example information from Twitter and Foursquare has been combined, but what happens if data from Facebook and other various services of Google are joined? The combination possibilities seem endless. Moreover online privacy rules are changing and we are not aware enough.

6.1.2 Unmanned Aerial Vehicles

The colloquial term of a civil drone is defined by law as an unmanned aerial vehicle that is able to navigate and run autonomously without a crew on board. Some specially trained humans are able to remote this vehicle from the ground. [246]

6.1.2.1 Application areas of UAV

A drone has mostly negative connotations because this vehicle is often used in several combat missions in crises areas as well as war zones [247], but nowadays drones are used more and more intensively in civil ranges:

- movie productions and aerial photography [248]
- production and broadcasting of aerial footage [249]

[242] [Der13]
[243] [N.N15c]
[244] [Kar13]
[245] [Lec11]
[246] [Sol14]
[247] [Kot13]
[248] [Kot13]
[249] [N.N13a]

- surveillance of major events [250]
- exploration of inadequate areas of science [251]
- appraisal of water, storm and fire damage. [252]

This list could be continued without a problem and it shows that drones offer numerous potential and in some cases also alarming uses. The drone project of Amazon published in December illustrates that those thought experiments and "science fiction nonsense" really take on a concrete shape. Who else than Google and Amazon has the financial firepower to invest in such visions? In addition to the technical challenges which go hand in hand with this technology, the legal problems have also to be solved.

6.1.2.2 Legal response

On January 01, 2014 an important amendment to the Aviation Act came into force and it restricts in fact the application area; substantial regulation about privacy protection, however, cannot be found. The Aviation Act separates two classes [253] of unmanned aerial vehicles or colloquial called drones:

1. Unmanned aerial vehicles of the class 1 [254] have to be within the range of visibility of the pilot and it is not allowed to use them for commercial use. Furthermore it is necessary to have a permission from Austro Control GmbH or any other competent authority for those unmanned aerial vehicles class 1. [255]

2. Unmanned aerial vehicles of the class 2 [256] are allowed to be in use outside the range of visibility of the pilot and in contrary to class 1 it is also allowed to use them for commercial assignments. On the other hand there are stricter restrictions for the usage and the controlling person needs a pilot's license as well as a certificate which attests the airworthiness. [257]

When making photos, videos and audio files by means in the air the same rules according to the Data Protection Act 2000 [258] apply as on the ground. To that effect drone users of both classes have to comply with the requirements of data protection law [259] and a notification has also to be sent to the data protection authority before using the drone.

[250] [Kot13]
[251] [Sol14]
[252] [N.N13a]
[253] § 24 f and g Aviation Act, [Luf13]
[254] § 24 f Aviation Act, [Luf13]
[255] [N.N13b]
[256] § 24 g Aviation Act, [Luf13]
[257] [N.N13b]
[258] DSG 2000, BGBI. I Nr. 165 / 1999
[259] §§ 7 ff in combination with § 6 and §§ 50a ff DSG 2000

6.1.3 Google Street View

Google Street View is a service free of charge and online available from Google Inc. This popular service is an extension of the already longer existing Google Maps service and enables a 360 degree view for selected cities and landscapes. [260] The data for this view is determined with a camera which is installed on the top of a car. [261] Many people use this service to get a virtual glimpse of the environment before starting a journey to that location: a nice-to-have-feature, which is of course not offered by classical travel guides. [262] In 2010, Google sent cars with cameras on the top trough Austria to digitalize the streets and roads. [263] The pictures that go online are snapshots of the reality, but it is not a live broadcast. Nevertheless, the risks are present, that potential burglars use this particular service for spying out residential areas (cf. chapter *Pleaserobme.com*). Shortly after, the Austrian data protection authority prohibited the Street View Service because during this journey through Austria not just photographs were taken but also data about WLAN networks have been determined without permission. [264]

6.1.3.1 Legal reactions

Decisive for the applicability of the Austrian legal order [265] is not the location of the server (Google Inc. in the US) but the location of the client (user of the Street View service). The client uses data and sets logical connected steps of usage by benefiting from the offer on the server [266]. Finally, DSG 2000 is applicable as far as the access on Google Street View is performed from the domestic territory. [267]

Since April 2011 Google Street View is registered in the data processing directory. The data protection commission has pronounced three recommendations to Google Inc. whereof point 1 and 2 in the following list have to be realized before publication of data in the internet. The third recommendation indicates that this regulation has to be realized 12 weeks before the publication of the data in the internet. In the following section those three recommendations are pointed out:

1. In the course of the reporting respectively the inspection procedures [268] Google has already assured to disguise faces and license plates. [269] When taking pictures of people in sensible areas like in front of churches, prayer houses, hospitals, women's refugees and prisons, not just faces but also the overall picture of the person has to be disguised. [270]

[260] [Kno10], p.16
[261] [N.N11b]
[262] [N.N14c]
[263] [N.N11a]
[264] [Bun10c]
[265] [Kno10], p.16-17
[266] cf. §4 Clause 7 DSG 2000
[267] § 3 Section 1 DSG 2000
[268] § 30 DSG 2000
[269] [N.Nb]
[270] [N.N11a]

2. Pictures of private properties not observable for pedestrians like particularly fenced private gardens and courtyards have to be disguised before the publication of data in the internet. [271]

3. The person concerned has the right to object from the point of determination of the data. [272] Before the publication of the image, the concerned party has to be given the chance to exercise the right to object in order to prohibit the publication of images from properties and buildings. Therefore suitable tools have to be provided which enable a simple and unbureaucratic assertion of the right to object. [273]

Those three recommendations are too strict and severe for Google Inc, wherefore the service of Street View has not been activated in Austria to the full extent, with one exception, namely "Special Collections". "Special Collections" include for example the "Hanappistadion" [274] and some ski slopes in Sölden and Ischgl. [275]

6.1.4 Zombie-Cookies

Turn is one of the largest advertising and tracking companies, which implemented an alarming tracking method provided by Verizon to respawn deleted cookies on mobile devides. They mainly use Real-Time Bidding, where free advertising space for a few minutes is auctioned within milliseconds. Displaying the advertisements whilst loading the web page is a major advantage of this controversial technology. [276] Jonathan Meyer, a computer scientist and lawyer of the University of Stanford calls these cookies Zombie-Cookies and authored an comprehensive article on his own blog [277] Within this article he mentioned that there are two ways to track a user with the Verizon header. The beforementioned zombie-cookie is the transparent way of tracking, because (1) the header is only attached to existing cookie tracking and (2) in case of missing cookie ID of a user it is reconstructed from the Verizon header. This first way is the well known zombie cookie. Apart from that the detection of the more devious way of using surreptitiously values on the backend is quite difficult. [278] Because of using Unique Identifier Headers (UIDH) of Verizon, Turn's zombie cookie is immediately restored once it is deleted by the user of a Smartphone. Turn.com, however, offers a so called opt-out cookie on their website, but even if this cookie is set and the additionally offered opt-out functionality of Verizon is occupied, the Zombie cookie reappears. [279]

[271] [N.Nb]

[272] § 28 Section 2 DSG 2000

[273] Google Inc. must prod to the right to objection as well as to the tools for exercising this right of objection on the website.

[274] [N.N14g]

[275] [N.N12a]

[276] [Tho15]

[277] cf. `http://webpolicy.org`

[278] [Mey15]

[279] [Tho15]

The Electronic Frontier Foundation investigated several common mobile browsers and privacy apps in respect of the features to protect against Verizon. [280] Common examples, such as AdBlock, Chrome, Firefox and Safari, were installed in their default configuration and tested according to Turn's ability to respawn the deleted cookies. It turned out, AdBlock (Platform Firefox for Android) and Safari (Platform iOs) are able to protect against Turn's invasive user tracking, whereas Chrome and Firefox are not. [281] Pursuing the advice in Verizon's privacy policy, full protection can only be guaranteed, if their product is not used at all. [282]

6.1.5 ELGA

The *Working Community Electronic Health Record* has released the following definition: "The electronic health record includes all relevant life, multimedia and health-related data related to a uniquely identified person. The data and information sourced from various health service providers as well as the patients themselves are stored in one or more different information systems, so called virtual health records. They are available in an appropriate processed form at the point of care among all eligible persons according to their roles and the legal conditions of data protection, independently of location and time." [283]

6.1.5.1 Data Protection

In its opinion, ARGE ELGA concluded that ELGA does not correspond to the data protection regulations in Austria. [284] Apart from the aspects, which are already discussed in *chapter Austrian law*, the right of individual citizens, including right of access, correction of inaccurately recorded data and cancellation of data processed unlawfully, are defined in the Data Protection Act 2000. In addition, the consent of affected individuals has to be obtained according to current Austrian law. Every citizen must be able to obtain information about personal data processed; therefore it is necessary to log all accesses to data. Sensitive data, such as personal and health data, are defined in § 4 (2) DSG 2000 [285] and classified as particularly vulnerable. In the context of healthcare, the usage of sensitive data does not violate the legitimate secrecy interests, unless healthcare professions dealing with these data are bound to confidentiality secrecy. [286]

[280] [Eck15]

[281] [Eck15]

[282] "If you do not want information to be collected for marketing purposes from services such as the Verizon Wireless Mobile Internet services, you should not use those particular services." [N.N14e]

[283] [Mag11a], p.342

[284] [ELG06]

[285] [DSG14]

[286] [Mag11a], p.343–344

6.1.6 Sexting

On the occasion of the 12th International Safer Internet Day on February 10, 2015 a study on Sexting [287] was published by Saferinternet.at. This study was carried out in the period between November and December 2014 and included interviews with 500 Austrian adolescents. The word "Sexting" is made up of the words "Sex" and "Texting". [288] The initiative Saferinternet.at describes Sexting as sending and exchanging of own nude photographs via internet and mobile phones. The most popular tools for sending and exchanging are WhatsApp, Facebook and Snapchat, but nude shots are also uttered via Skype and Kik. [289]

Saferinternet.at supports not only kids and teenagers but also parents and teachers in using the internet in an appropriate safe way and furthermore Saferinternet.at provides lot of helpful advice about social networks, data protection, youth protection, computer/video games, online shopping etc. The initiative is coordinated by the Austrian institute for applied telecommunication (ÖIAT) and by the association of the internet service providers Austria (ISPA) and is realized with the collaboration of NGOs, economy and the public authorities. [290]

[287] "Sexting in der Lebenswelt von Jugendlichen", [N.N15a]
[288] [N.N12b]
[289] [N.N15a]
[290] [N.N15b]
[291] [N.N15a]

51 % of the young people questioned, know someone who has already taken a nude photograph of himself/herself and sent it to other people.	16 % of the young people questioned have already made a nude "selfie" and circulated it.
33 % of the young people questioned have already received nude photographs.	81 % of the young people questioned see sexting as a potential danger which could have some unpleasant consequences!

Table 6.1: Four concrete numbers of sexting study [291]

The study identified the most important motives for making and sending these individual nude images, namely as means of self-portrayal in the social environment, as proof of love or even for getting to know each other and flirt. [292] As the table shows, surprisingly a lot of young people (81 %) classify Sexting as a real danger. The exposure by the distribution of the nude images in the circle of friends or on pornographic websites, extortion and also the prosecution due to a violation of the §207a StGB (*see chapter Current legal situation*) are just fractions of the risks which Sexting involves. Some precautionary measures to prevent a possible loss of control are shown in the study by experts from 147 "Rat auf Draht" and Saferinternet.at. [293] It is recommended to delete the photographs and images in regular intervals because smart phones are often borrowed to third persons or passed on to somebody else. To obtain control over the own pictures, those images and videos should not be dispatched but only be shown on the own mobile phone. [294]

[292] [Ste15]
[293] [Ste15]
[294] [Kro15]

6.1.6.1 Current legal situation

§207a StGB is actually used in the battle against child pornography but it also finds usage in context with Sexting. According to the current relevant legislation, underage persons are allowed to take pornographic nude photographs for themself and to keep them individually, but it is prohibited to share them with their friends or other people online. [295] To give an example: If young people, who are in a relationship, send their partners pornographic "selfies", they are punishable in accordance to §207a StGB. Numerous organizations in Austria demand a modification of §207a StGB, because the right of self-determined sexuality of young people is restricted/limited. ECPAT Austria, the consortium for protection of children against sexual exploitation, suggests a diversification between primary and secondary Sexting. Primary Sexting should just involve the creation and circulation of the nude pictures through the minor depicted, whereas secondary Sexting includes the circulation of the nude pictures through a third person. Thanks to this division it would be possible not to prosecute primary Sexting. [296] In my interview with a prosecutor I treated a concrete case of Sexting which I describe in *chapter Case 5 - Pornographic depiction of minors on page 77.*

6.2 Big Data

Big Data is, first and foremost, a large amount of data, which is either collected, made available and evaluated via the internet or somewhere else. Much of the data is related to a person and thus comprised for various uses, for example recognition of statistical trends. Moreover, Big Data offers chances and possibilities for new social, economic and scientific findings to improve living conditions within our complex world. Big Data also harbors new risks, like the abuse of power through manipulation, discrimination and suppression. The consolidation of big data amounts, done by public and private agencies can lead to a gross violation of fundamental human rights through exploitation. Big Data is one of the most important new technology driver in addition to cloud computing and is therefore examined in detail in this thesis.

6.2.1 Definitions

After combing through various sources, I would like to give some definitions of Big Data, since no definition takes all relevant aspects into account:

> Dan Kusnetzky defines the term "Big Data" as "tools, procedures and processes allowing an organization to create, manipulate and manage very large data sets and storage facilities." [297]

[295] [N.N15b]
[296] [N.N15d]
[297] [Kus10]

McKinsey&Company, a global consulting agency, announced Big Data as "the Next Frontier for Innovation, Competition and Productivity". [298]

The term big-data refers to analytical technologies that have existed for years but can now be applied faster, on a greater scale and are accessible to more users. [299]

NIST defines, in addition, "Big Data shall mean the data of which the data volume, acquisition speed, or data representation limits the capacity of using traditional relational methods to conduct effective analysis or the data which may be effectively processed with important horizontal zoom technologies". [300]

A widely used definition of the characteristics of Big Data comes from Gartner, the world's leading information technology research and advisory company. Gartner analyst Doug Laney introduced the 3-Vs concept in a 2001 Meta Group research publication. Gartner's 3-V-Model describes three dimensions of data growth and is part one of Gartner's definition. [301]

6.2.2 Gartner's 3-V-Model

The first dimension refers to the increasing volume of data. The second and most important dimension deals with data variety, whereas the third dimension, data velocity, has to be examined from two perspectives.

Part Two of Gartner's big data definition deals with cost-effective, innovative forms of information processing, especially thinking about technology capabilities to store and process unstructured data, linking data of various types, origins and rates of change and performing comprehensive analysis. [303] Svetlana Sicular, research director at Gartner, tells her clients that enhancing insights and, hence, making decisions is the ultimate goal and missing this part three, leads to tedious problems when identifying and formulating big data issues. [304] Before explaining the three dimensions of the 3-V-Model in detail, I want to instance Gartner's big data definition, which merges all previously mentioned essential parts:

[298] [Min14], p.2
[299] [Mil13]
[300] [Min14], p.4
[301] [Sic13]
[302] [Dom13]
[303] [Dom13], p.320
[304] [Sic13]

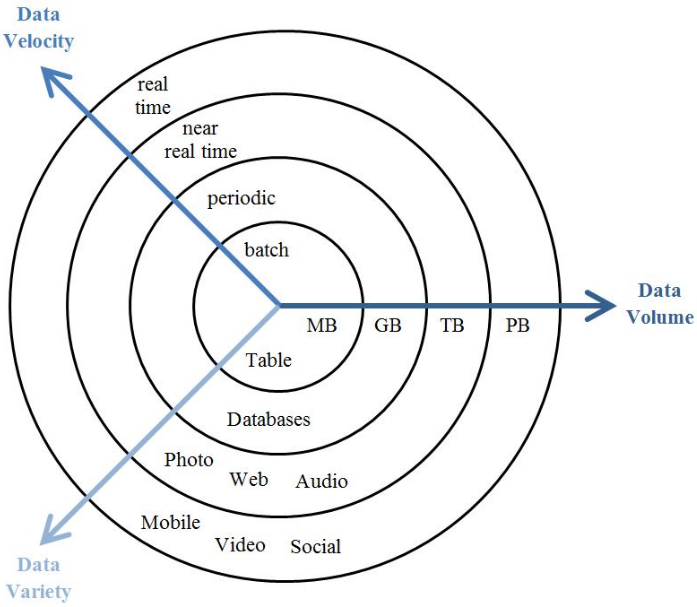

Figure 6.1: Gartner's 3-V-Model [302]

> "Big data" is high volume, - velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insights and decision making.[305]

6.2.2.1 Data Variety

I would like to start with describing variety, because the vast amount of data is the most important aspect in this big data definition. Variety refers to data from different sources and can represent variances such as type, format and structure (structured, semi-structured and unstructured data). Structured data, such as customer databases are stored in tables of traditional databases, where each row corresponds to a record. Although semi-structured data are partly structured, they have also an unstructured part. An example could be e-Mail messages, which consist of a header and a body. The header of a message is clearly structured, namely in a sender and a recipient or subject, whereas the unstructured body may contain any content or attachments. [306] Structure can no longer be imposed like in the past in order to keep control over the analysis.

As part of Big Data, all existing data, whether structured or unstructured, are summarized and analyzed together. The resulting unstructured data conglomerate can be classified into three categories:

[305] [Iaf14], p.26

[306] [Dom13], p.320

1. The first category contains results from person-to-person communication. As shown in the figure 6.1, data of social networks, video and mobile systems, as well as web log files may be possible examples.

2. E-Commerce applications, or more generally person-to-machine communications, generate data that can be assigned to the second category.

3. Machine-to-Machine communications, such as sensor data, GPS data or surveillance images, can be identified as third category.

The real world has got data in many different formats and that is the challenge we need to overcome with Big Data mechanisms.

6.2.2.2 Data Volume

The Internet Giant Google receives over four million search queries and e-Mail users send over 200 million messages every minute of a day. [307] The emergence and widespread popularity of social networks on the internet is changing by the way we live and work. Recent reports from the market research company Nielsen indicate that social networking and blogging are the most popular activities on the internet worldwide. One of the most prominent and probably biggest social networks, Facebook, claims to have more than one billion users worldwide, whereas these users share 2 460 000 pieces of content every minute. [308]. To illustrate the massive amount of data offering chances of misuse, the following examples are provided: "Google processes more than 24 petabytes of data per day, a volume that is thousands of times quantity of all printed material in the U.S. Library of Congress. Facebook, a company that did not exist a decade ago, gets more than 10 million new photos uploaded every hour. Facebook members click a "like" button or leave a comment nearly three billion times per day, creating a digital trail that the company can mine to learn about user's preferences. Meanwhile, the 800 million monthly users of Google's YouTube service upload over an hour of video every second. The number of messages on Twitter grows at around 200 percent a year and by 2012 had exceeded 400 million tweets a day." [309]

Quoting the rough estimation, that the now available amount of data will double every two years or thinking one step further in 2020, we well have 50 times the amount of data as exists in 2011.

6.2.2.3 Data Velocity

The pace at which data flows in from several sources, like human interaction in social networks, business processes and industrial mechanisms, is called data velocity. [310] Moreover, data velocity refers to the almost unimaginable speed at which the data is

[307] [Dom13]

[308] [Jam14]

[309] [MSC13], p.8

[310] [Nor13]

generated, stored, analyzed and delivered [311]; however, this data collection and analysis must be timely and rapidly conducted for reasons of maximizing commercial value of Big Data. [312]

For the sake of completeness, however, I describe the remaining four V's, namely veracity, value, variability, visualization, within the next four short sub-chapters.

6.2.2.4 Data Veracity

The challenge of data veracity is to overcome the biases, noise and abnormality in the data resulting from various different sources. [313]

6.2.2.5 Data Value

Data Value simply represents the business value for organizations, societies and consumers, which can be derived from Big Data. Data in itself is not valuable, but the data value appears while analyzing that data as well as turning it into potentially profitable knowledge.

6.2.2.6 Data Variability

The additional dimension "variability" is often confused with "variety". To demonstrate the difference I introduce a simple example: A bakery sells ten different breads. That is variety. In contrast, variability is when you go to this bakery ten days in a row and every day you buy the same type of bread but it tastes and smells differently each day. [314]

6.2.2.7 Data Visualization

A big technological challenge of visualization is to present the vast amount of data to the general public in a transparent and comprehensive way.

6.2.3 Big Data Types

According to Sylvia Frühwirth-Schnatter, [315] the distinction of two big data types, namely "tall and skinny" and "short and fat" is an interesting aspect of Big Data analysis. These two types differ with respect to the observation units and the individual nature of the data. [316]

[311] [Dom13], p.320
[312] [Mar14a]
[313] [Nor13]
[314] [Mar14a]
[315] Department of Statistics and Mathematics at the Vienna University of Economics
[316] [Chr14], p.4

6.2.3.1 Tall and skinny

"Tall and skinny" means that lots of observation units are present in a few individual data, whereby many important variables are often not recognized. A labor market project of Frühwirth-Schnatter analyzes the influence of the length of parental leave on the subsequent chances of mothers in the labor market. In this particular example there are data from hundreds of thousands of mothers, but without indication of part-time or full-time employment. [317]

6.2.3.2 Short and fat

The second type, namely "short and fat", considers few observation units with individual data, such as analyzing genetic data. In this case it is necessary to filter out the relevant information from the wealth of data using statistical methods, Frühwirth-Schnatter emphasized. [318]

6.2.4 Loss of Control

Big Data totally undermine the data protection. The recipients of the data shall be bound by the purpose limitation principle - i.e. data may only be processed for the purpose for which it was originally collected. The data subject should be informed about the purpose of collection, processing and use of data. Article 6 Section 1 (b) of Directive 95/46/EC determines the purpose limitation principle as a fundamental principle of any data processing. [319] [320] When applying big data technologies, data is taken out of their original purpose, brought together from different areas, evaluated, structured and applied to new uses. [321]

[317] [Chr14], p.4

[318] [Chr14], p.4

[319] [Dr.15]

[320] 1. Member States shall provide that personal data must be:
a) processed fairly and lawfully;
b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
c)adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

[321] [Joc]

6.3 Web-Tracking

Mass surveillance and espionage by government organizations such as secret services have been intensively discussed in public since the revelations of Edward Snowden. Not only secret services collect data from citizens, but also companies gather information from consumers without their knowledge. Web-tracking is an effective method for gathering and accessing personal data, whereas consumers are persecuted by third parties in the World Wide Web. Web-Tracking is far more than just data ascertainment, it includes also the storage, usage and the exchanging of data about the individual online behavior. In case of using Cross-Domain Tracking it is also possible to track a user on websites of multiple vendors. Consumer data, such as consumer behavior, political attitudes, personal interests, age, relationship status, lifestyle and various other private information of users are an important input for many companies. These data are collected by web-tracking methods and furthermore used for target advertising. This whole amount of data can be used to detect the different interests, political opinions or even diseases of every individual user. Searching a present for somebodies birthday via an online-store, googleing an address, planning the next journey in the upcoming summer via an online travel portal and after that organizational staff ordering food via an online delivery service – all those activities are leaving marks in the internet which can be easily recorded with special Web-tracking-tools. Web tracking is not only a basis of decision for private persons, business related decisions are also made on basis of collected and recorded customer profiles. [322] The most famous and market-leading Web-tracking service is Google Analytics. This service records without special consent and often also without knowledge of the user personal and individual data. [323] Target advertising is only one possible application for consumer data, because they can also be used in various business models:

- search engines
- cloud and hosting services
- E-Mail and web services
- online word processing
- content offers

The advertisers have to collect as much information about each individual customer as possible to offer individual advertising on websites. Advertisements are not longer based on the contents of a loaded page, but on the user information collected by the advertiser.

Technical abilities for recognition of the users can be divided in two different classes namely explicit tracking and closing tracking. Trackers are able to use several tracking

[322] [Int13], p.7
[323] [Rol08], p.324

methods at the same time but experts are also developing constantly new methods for uni-vocal recognition of as many users as possible.

6.3.1 Explicit tracking

When using the method of explicit tracking [324] the trackers transmit data to customers computer. Those transmitted data is stored on those computers and can easily be retrieved at a later point of time. The most famous examples are third-party-cookies, flash-cookies, e-tags, HTML5-Storage and evercookies, whereby I am going to concentrate on third-party-cookies in the following section: Third-party cookies come from other websites' advertisements (such as pop-up or banner ads) on the website that you are viewing. This applies typically for advertisement which is supplied by third parties suppliers or for social widgets like the Facebook like button. [325] Third-party cookies are placed in a way that a site can remember surfing and personalization preferences and tracking information about various persons at a later time.

6.3.2 Closed tracking

Contrary to explicit tracking with this method there are no data transmitted to the customers computer. Trackers try to distinguish those computers by configuration aspects and system properties. Examples for closed tracking [326] are on the one hand the tracking of IP addresses and on the other hand the so called browser or system fingerprinting.

6.3.3 Impact on consumers

In connection with the ascertainment of data the Fraunhofer-Institute for secure information technology (SIT) speaks about the formation of further data sources through the internet of things, which are in further consequences combined with already collected data from other Web-Tracking services. Not only the internet of things has its influence there, the internet of services and of course cloud computing provides further usable data of customers. As mentioned before the diversity of data sources enables to get a glimpse on patterns out of various technologies by using Big Data technology. Customers can be divided in categories according to their similarity. By processing the data the profiles of persons which are extracted by Web-Tracking can be linked with real identities of the affected persons whereby the borders of the online world are already crossed. The next step after the creation of those personal profiles is the analysis of social relationships based on those profiles. [327]

The exploitation of person related data is a lucrative business. The magazine "Profil" headlined among other things "data is the new oil"; [328], not only the trading of data is a

[324] [Mar14b], p.9
[325] [Ach13]
[326] [Mar14b], p.9
[327] [Mar14b], p.11–12
[328] [Seb13]

lucrative business, but also new business models keep the cash registers ringing. The loss of control is imminent when data is transmitted deliberately or even gets stolen and lands at organizations which are declined by customers. Acquisition of companies and the wide distribution of trackers enable the creation of complete customer profiles. A lot of customers do not even have the knowledge about this particular danger of tracking. This is why the impacts of those attacks cannot be estimated correctly and why there are no tools installed for tracking protection. It is virtually impossible to get usually collected data deleted.

6.3.4 Impact of losing control on individuals

Web-Tracking is a risk which does not affect only individuals it's also a real threat for the entire society (community). Not only economic disadvantages can arise, but also threats and risks for sentimental values. I want to divide the following factors of influence in two separate categories:

6.3.4.1 Threats for sentimental values

The pursuit of customers in the World Wide Web can to a certain extent be compared to stalking. In this context I want to mention the real stalking case which I illustrated in *chapter Real-life examples of losing control on page 69*.

In the broadest sense tracking affects the freedom and self-determination of persons, because when the user becomes aware of the tracking risk, he might conduct a little bit different in fear of the consequences as if he had no knowledge about the tracking itself or the deployment of tracking. In the United States there are information services where everybody can get specific data like the household income, marital status, education, hobbies, interests and the value of the property possession from specific persons via the internet. [329]

Tracking restricts not only the freedom of those persons, it creates opportunities to manipulate customers. For example, two persons run the same search query via Google: it is possible to get two different results due to the saved search history. Furthermore tracking affects the freedom of press and leads to the literally extinction of print media (newspapers), because they are not able to match this target-oriented advertising over the internet. Opinions and attitudes of single persons can spread so rapidly and develop a separate momentum which can lead to terrifying consequences.

6.3.4.2 Threats for material values

Price discrimination in online stores can lead to an economic disadvantage for the customer. In a self-test Florian Stahl, professor of quantitative marketing at the University of Mannheim, considered a hotel via booking.com. He logged off, deleted the cookies of his browser and started the enquiry again and he suddenly got an offer where the same

[329] [Mar14b], p.11–12

room was much cheaper than in the previous experiment [330]. Depending on the financial status of the clients which are known via tracking, different customers are offered the same product or service at different prices.

The price has long been a stable size for customer orientation and comparison purposes. Prices get dynamic, individualized or even completely replaced by auctions by means of dynamic pricing mechanisms. Already in 2000, Amazon offered their customers different prices for the same product at the same time. Dynamic Pricing is known from auction platforms and online stores, but is more and more used in stationary trading. The technological progress makes it possible (1) to implement time dependent price staggering, (2) to fluctuate the price depending on supply and demand or to (3) perfectly adapt the prices to the customer needs. The willingness to play of individuals could not have been determined up to now, but nowadays the analysis of huge amounts of data makes it possible. Economists talk about a "first degree price discrimination", wherein each customer pays its own price for the same product. [331] Factors influencing the dynamic pricing can be:

- Browsers and devices: If a website is visited of a user having an expensive Macbook, the price increases. Customers who rely on online trade have to pay more, because of the fact, that the determined location is not close to a store. [332]

- History of surfing behavior: Impulse buying is much more expensive than previously collecting information about the product in the internet. Again, Google is strengthening its pioneering role: In 2012, Google has applied for a patent on it to use dynamic pricing for electronic content (e-Books or online videos).

[333] The mail order company "Otto" is already working together successfully with a service for dynamic price management, namely Blue Yonder [334]. In France, electronic price tags are found in almost every major supermarket and also in Germany retail chain stores, Kaufland and Netto, work with dynamic prices. [335]

Furthermore, departments of personnel are using the World Wide Web as source for information about the applicant (candidate). The recorded data from tracking (attitudes, habits, preferences, aversions, abode, medical condition or state of health, financial and professional situation, social relations, consumer behavior, wishes, etc) are of great economic relevance in this context.

I see the usage of data from social networks as a significant intervention to privacy for the calculation of granting a credit. More and more frequently companies are arising from the dark who offer service for assessment of creditworthiness.

In my mind even more serious seem the effects of web-tracking on the health system. In the future the following questions have to be asked by the customers themselves:

[330] [Han14]

[331] [Pas15]

[332] [Pas15]

[333] [Pas15]

[334] http://www.blue-yonder.com/

[335] [Pas15]

(1) Who has access to my data if I document blood glucose, blood pressure, pulse and the daily amount of steps in an app on my smart-phone and (2) who, except from my personal friends on Facebook, has access to my data (maybe my doctor, the health insurance company or even Amazon)? Due to a survey of the Fraunhofer institute of secure information technology, 72 % of the smart-phone apps are using web-tracking framework. [336] There are a few known cases where health insurances fall back on collections of customer data to evaluate the health risks of the individual customers for increasing the fees.

[336] [Mar14b], p.10

6.3.5 Protective Measures

This chapter lists a number of protection tools against Web-Tracking. On the one hand it is possible for the customer to protect himself via tools which are already included in the browser and on the other hand there are browser add-ons available which can easily be installed. New Web-Tracking methods are constantly being developed, but there is still some advice available about protection from cookies and other common methods.

A simple but truly effective method is to block cookies or to delete them after every internet session. One disadvantage is that some websites are not displayed correctly and therefore exceptions have to be defined. [337]

Using the private mode gives protection in respect of over other persons who are using the same device. For example a history of the accessed websites will not be created and the usage of cookies is also seemingly disabled. Nevertheless in practice data collectors are able to circumvent the so called "Do-Not-Track" settings.

In September 2011 the World Wide Web consortium (W3C) founded a Tracking Protection Working Group [338] which is working on a "Do-Not-Track"-Standard (DNT). Their mission is to improve user privacy and user control by defining mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web-Tracking elements. Following the Do-Not-Track Standard a flag is shown to the tracker and that means the user does not want to be tracked. Insofar the customer is reliant on the trackers' willingness to cooperate. [339]

By means of Tracking Protection Lists (TPLs), the browser can completely block connection establishment to the tracker given that the tracker is on that list. [340]

The Fraunhofer SIT developed a crawler on behalf of Microsoft; this tool searches in an interval of a few days for trackers on popular sites and the identified trackers are then put on the tracker protection list. [341] This blacklist mechanism is implemented in the Internet Explorer by Microsoft but it can easily be installed onto other browsers as well. [342] Internet Explorer 9 is at least necessary to be able to use Tracking Protection Lists.

After the installation of the TPL the protection against various different tracking methods is activated and new tracking methods are handled easily by the automatic download of the updated TPLs.

In comparison to the Do-Not-Track Standard the protection by using Tracking Protection lists is better because the protection does not depend on the tracker's willingness to cooperate.

[337] [Mar14b], p.81-83

[338] `http://www.w3.org/2011/tracking-protection/`

[339] [Int13], p.10

[340] [N.N14f]

[341] [N.N14a]

[342] `https://www.sit.fraunhofer.de/de/tpl/`

6.4 Cloud Computing

Generally Cloud Computing is a form of outsourcing, as far as IT services are no longer carried out on own systems, but outsourced to service providers [343]. Cloud Computing as a further development of application service providing (ASP) does not offer a flexible model to process data and software locally, but rather in server farms, spreaded all over the world [344].

6.4.1 Concept and meaning of "Cloud Computing"

Hitherto there is no legal or generally accepted definition of Cloud Computing. To point out significant characteristics of Cloud Computing, however, I will quote the following definitions:

> "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [345]

> "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs." [346]

> "Cloud computing is an on demand service model for IT provision, often based on virtualisation and distributed computing technologies." [347]

6.4.2 Application scope of DSG 2000

Data Protection Act 2000 is objectively applicable if personal data, which means information about individuals whose identity is determined or determinable, is processed in the cloud. The processing of anonymized data or data used without reference to individuals is not subject of DSG 2000, however, other regulations must be taken into account. In many companies data is processed for different purposes, such as accounting and financial

[343] [Mar12]

[344] [Rai11]

[345] National Institute of Standards and Technology, [PM11]

[346] https://www.research.ibm.com/haifa/projects/systech/reservoir/public/CloudDefinitionPaper.pdf, [Lui]

[347] [Dan09], p.14

data, product and sales data, e-mail correspondence, personnel data, trade and business secrets as well as transaction data [348]. These data can either have a personal reference to the company or to customers, suppliers or employees of the company [349]. Moreover, the Austrian Data Protection Act is applied, if the client is incorporated in Austria and the data is processed domestically. The degree of protection of processed data depends on the data categorization and determines the scope of data security measures. Accordingly, the processing of sensitive data is subject to higher requirements than the processing of non-sensitive data.

6.4.2.1 Data subjects in Cloud Computing

The general definition of the data subject is already discussed in *chapter Austrian law*. However, personal data can be customer and employee information, vendor data or other data within the scope of a business relationship. The obligation of the cloud user is to protect the secrecy interests of the data subject and the rights to access, correction and deletion of data as well as the right of opposition, which is often difficult to provide correctly regarding to the cloud structure. [350]

6.4.2.2 Controllers in Cloud Computing

Cloud Computing distinguishes between Cloud providers and Cloud users, whereas the provider and the controllers are in a civil law contractual relationship. The controller is taking the chair of an end-consumer by using the Cloud service for the own advantage or as entrepreneur who offers this service to other consumers. In both cases the cloud user is to qualify as a controller according to §4 (4) DSG, because he has made the decision to use the data for the own advantage or to hire a processor. In such cases the cloud user leaves some parts or even the whole data stock to the provider. [351] This is called data surrendering [352], whereas the precise definition of data surrendering as well as the extensive legal duties of the controller are explained in *chapter Definitions of personal data*. For practice it is essential that the cloud user still owns the data and he is always responsible for observing the legal provisions of DSG 2000.

6.4.2.3 Processors in Cloud Computing

The detailed definition of a processor according to §4 (5) DSG is located in *chapter Processor*. According to this definition the processor has to act only upon instruction of the controller. That means that he is receiving the data just for carrying out the instructions without getting any special legal authorization. The cloud provider is storing or processing user information just in a technical view and is registered as a processor.

[348] [Rai11], p. 563

[349] A distinctive feature of the DSG 2000 is not only the protection of individuals but also of legal persons or groups of persons

[350] [Mag11b], p. 61

[351] [Mag11b], p. 59

[352] §4 (11) DSG

The term "work" is often used in an ambiguous way, because it includes not only the achievements of a civil law contract for work [353], but also automation-aided achievements. In this connection two further concepts are to be mentioned: data usage and data transmission is already explained in *chapter Definitions of personal data.* With regard to cloud-based services it has to be checked whether the provision of services by means of software, platforms and infrastructure is actually a data surrender for a performance of a work. In addition, it should be noted that the Data Protection Commission is [354] in favor with the processor term concerning hosting websites and the ASP. This has the advantage that the strict conditions of the section §7 Section 2 DSG 2000 must not be fulfilled, because it is not a data transfer, just a mere information sharing. This privilege applies only within Austria, the EU or EEA. Simple information export into foreign countries according to §12 Section 5 DSG 2000 is subject to stricter admissibility criteria according to §7 Section 2 DSG 2000 and there have to be further examinations [355] if the receiving country has an adequate data protection level. Cloud Providers act usually by outsourcing to other resource providers, if the own resources are exhausted. Large providers fall back on own company-based data center, while smaller providers fall back more likely to sub-enterprises. Moreover, the DSG 2000 contains no legal definition of a "sub-processor" therefore the transmission of data between a processor and a sub-entrepreneur is to qualify as a simple information sharing.

6.5 Video surveillance

6.5.1 The right of access to data

Persons, who are captured of videocameras in everyday life have, according to certain specifications, the right to get insight into the video surveillance material. This right of access is enshrined in the Austrian Data Protection Act 2000 and serves here above all to create transparency. It offers affected people the possibility to revoke the asymmetry of monitoring, even though it is only for a short term.

6.5.2 Legal situation in Austria

Because of the fact that video surveillance usually processes personal image and video data, the fundamental rights of privacy [356] and data protection [357] are applied. In Austria the legal situation of video surveillance is mainly governed by the DSG, especially in section 9a. There are two other noteworthy legal sources concerning video surveillance. First, video surveillance by the police is regulated in the Security Police Act and second there

[353] §§1165 ff ABGB

[354] Decision K120.819/006-DSK/2003 from 14.11.2003

[355] §§12 and 13 DSG

[356] [Bun10a]

[357] [DSG14]

is the regulation of copyright questions within the Copyright Act [358]. Video surveillance is subject to the legal obligations for the data processing register pursuant to §§17 ff as well as 50c DSG. Moreover, marking obligations of monitored areas are established in §50 d DSG [359]. One exception of labeling requirements and the obligation to register is real-time monitoring. Real-time monitoring is video surveillance via live broadcast without data storage as well as analog video surveillance. According to §50 b DSG 2000 [360] stored video data need to be deleted after 72 hours. Everyone, having appointed time and place, and proof of identity, has the right to get information about the processed photography and video recordings [361]. The operator of a video surveillance system has to cause the transmission or delivery of a copy in a generally accepted technical standard [362]. Video data must not be deleted since the date of request for information is known [363]. In case of failing to supply information, the applicant is entitled to get a written description of the processed behaviour or visual information when defacing other people [364]. The information has also to establish the recipients or groups of recipients of the data, the purpose of data usage as well as the legal bases in a generally understandable form. All replies to requests must be answered within eight weeks [365] and once a year gratuitously [366].

[358] According to §78 Section 1, portraits of people may be neither publicly displayed nor publicly distributed, if the material interests of the person depicted or those of close relatives get infringed. [Bun10b]

[359] [Rob14]

[360] [DSG14]

[361] §§26 and 50e DSG 2000

[362] [Rob14]

[363] §26 Section 7 DSG

[364] §50e Section 2

[365] §26 Section 4 DSG 2000

[366] §26 Section 6 DSG 2000

CHAPTER 7

Real-life examples of losing control

This chapter describes the processed contents of the interviews with a prosecutor, which are combined with theoretical concepts and lodged with legal implications. The first two legal cases deal with the offense of abuse of fraudulent data processing. Following this, I describe a case of assiduous persecution. The content of case 5 is a very current one, namely the problem of pornographic depiction of minors. Case 6 is related to aggravated assault. The interviews illustrated the current prevalence of my chosen topic.

Due to lack of translation of an official authority, excerpts from the Criminal Procedure Code, the Penal Code and the Juvenile Court Act are listed in addition in German language.

7.1 Case 1 - Fraudulent abuse of data processing

Suspicion: An unknown group of offenders seemed to have infected the mobile phone and computer of the victim by installing malware on those devices. Finally they made numerous withdrawals from three different accounts of the victim. They caused damages in the amount of approximately 20.000 Euros. Time of the crime July 16, 2014 – July 19, 2014

↓

The victim filed a complaint by telephone, after he discovered some mysterious withdrawals on his account. The police was taking evidence in this case.

↓

The regional CID (Criminal Investigation Department) has own experts for the internet. Those experts performed some internet research. It was detected, that the telephone number probably comes from the Ukraine. They got this information with a relocation of call data. Mobile phones and or computers of diverse victims in Austria got infected. The commission of the offense took illegally transaction numbers by using automation-supported data processing and they made withdrawals on the accounts of the victims. Paysafe cards were bought by the offenders and they took advantage of those cards in several online shops. They caused damage in the amount of 55.000 Euro to the previously known victims. It was again and again the same method of stealing money, because of that fact it was assumed that there is a professional organized group of offenders behind that crime, it was also assumed that a commercial commit of crime was the force for those offenders.

In the event report of the police it is requested to order the interception of messages and communication of information of data to identify the perpetrator. This so called recording of call data should provide relevant conclusions concerning the number of the perpetrator to which the TAN's were sent.

↓

The event report of the police is dedicated to the prosecutor's office Innsbruck with suspicion of fraudulent data processing abuse against unknown perpetrators. [367]

↓

The case covers Austria in total, therefore the whole investigation was extended to be able to investigate more affected persons. Results of the investigation are expected to be unveiled in February 2015. (Evidences will be collected) Since it is an ongoing process, there is no judgment.

[367] §148a StGB (1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, daß er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflußt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Wer die Tat gewerbsmäßig begeht oder durch die Tat einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen 50 000 Euro übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

7.2 Case 2 - Fraudulent abuse of data processing

The injured party filed a complaint [368] because his wife recognized on the 29.01.2014 that there were missing 3500 Euro on the common account. The remittance went to a Spanish account (financial institution in Bilbao) although the account holders did not authorize such a remittance. After consultation with their bank their account was immediately closed. It has been levied that the victim has made payments using e-banking tools and requested the required TAN codes via SMS up to this day. The male victim wanted to switch to a TAN list, instead of using the possibility to get the TAN codes via SMS. Exactly on that day, when the victim wanted to make this change, it was nevertheless possible for the offenders, to gain access to the bank account of the victim and change the cited telephone number, which is used for requesting TAN codes via SMS.

↓

Offence: An unknown offender has gained access to the e-banking account of the victim and changed the phone number of this account in order to use the possibility of requesting TAN code via SMS to transfer money (3500 Euro) to an account in Spain. Since IBAN and BIC is known, an adjudication of account opening could lead to the identity of the accused person(s).

↓

An arrangement of account opening and the transmission of master data by the prosecutor's office took place so that via the telephone numbers used by the offender more information was collected and analyzed. By analyzing that arrangement it is apparent if the direct debit was made by TAN or SMS, list of TAN's, letters or a so called "Verfügerkonto" in German. The time and the transaction number are also evident. In most cases the transaction number is very useful, because it is required to show an ID when you collect money abroad with a special transaction number.

In contrast to Case 1 the account opening purely refers to the account and not to the recording of call data.

↓

The order could not be executed in Austria because the account of the offender was opened in Spain. The Spanish authorities were asked to execute the order of opening the account and transmit the master data. Account information like owner, person who opened the account, time of the account opening, personal information about the account holder etc. often provide information about the offender. Note: It is not uncommon that offenders use falsified legitimation documents!

After the telephone number of the offender was identified the voice carrier was contacted. Details of a concrete subscriber connection, including the voice carrier, the time of the crime for verification and giving information is absolutely necessary. By

[368] §148a StGB, see also Case 1 - Fraudulent abuse of data processing

specifying the time of the crime the data volume can be limited and the evaluation is facilitated. The voice carrier is providing the following data for traceability: traffic date, access data including the announcement of the master data, the IMSI number and the IMEI number as well as the data of the roaming partner in connection with international calls and stays abroad.

↓

The case is still open because the results of the arrangement, which is carried out in Spain, must be awaited.

7.3 Case 3 - Assiduous persecution (Stalking)

On 02.09.2014 the victim made acquaintance in the social network with "Emrah". They chatted about trivial things until "Emrah" accused the victim to have sexual problems. The victim and "Emrah" had no contact via telephone but just with Tango and WhatsApp. She did not stand to that insult and sent pictures as evidence where she was shown in a nightdress and with her husband. "Emrah" has again contacted the victim via WhatsApp and SMS and wanted to meet her.

↓

On the next day "Emrah" created a profile of the victim on Tango including name, mobile number, intimate photos and facial images (based on the contact in which "Emrah" yearned for a personal meeting) and contacted several men in her name.

↓

The victim turned to the police and filed a complaint against an unknown person (obviously with the wrong name "Emrah"). In the period of September 2, 2014 until September 10, 2014 the offender arranged personal contact with the victim for third parties by using person related data of the victim. In the profile on Tango the first name of the victim was shown and also her hometown Innsbruck, but also her mobile phone number, intimate pictures from her body and also a facial image. "Emrah" did not make any threats against her. In the time of the crime 40 unknown male persons got in contact with the victim via WhatsApp, SMS and Tango. Those persons got attracted by the function of "wink somebody" (caused by the offender) which came from the offenders created pseudonymous profile on Tango. By means of the executive it was tried to find out in Tango who the offender was, but those investigations were not successive. In the meantime the victim changed her mobile phone number and it has since been no longer harassed.

↓

Case was closed. In order to satisfy the facts of §107a StGB [369], the offender must proceed persistently. On the one hand, the persistence of the behavior continuing despite setbacks

[369] §107a. (1) Wer eine Person widerrechtlich beharrlich verfolgt (Abs. 2), ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.
(2) Beharrlich verfolgt eine Person, wer in einer Weise, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt

1. ihre räumliche Nähe aufsucht,
2. im Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels oder über Dritte Kontakt zu ihr herstellt,
3. unter Verwendung ihrer personenbezogenen Daten Waren oder Dienstleistungen für sie bestellt oder
4. unter Verwendung ihrer personenbezogenen Daten Dritte veranlasst, mit ihr Kontakt aufzunehmen.

and failures is typical for those offenses and on the other hand this depicted behavior must occur over a prolonged period of time. As a guideline for severe cases [370] a minimum period of one month and at least three individual actions could be considered. [371] In the present case, the behavior lasted only a few days (September 03, 2014 - September 09, 2014). Since the profile of the offender had been deleted due to a telephone conversation with the husband of the victim, persistence of the behaviour of the offender could not be fixed.

[370] §107a StGB Section 2 Clause 3 as well as Clause 4

[371] Schwaighofer in WK2 §107a StGB Rz 10

7.4 Case 4 - Criminal dangerous threat

In this case, at a first glance no loss of control over personal data exist. Nevertheless the emotional loss of control and the aspect, that the threats were made by Facebook let the case still be interesting and relevant for my thesis.

A 16 year old pupil had apparently threatened other persons with death under the influence of his exclusionary state of sanity based on a mental or psychological deviance and he had put those persons into fear and agitation. This 16 year old was blameless until 2010, at this time he caught the eye at school with a physical assault against another student. The offender had previously announced some death threats to other people in his environment. The service of school psychology got involved in previous incidents.

↓

In a chat history on Facebook with a student of the same age the offender announced that he would hope to be in a good mood an Monday the February 27, 2012, otherwise it could get really "uncomfortable" for the chat partner and approximately 100 other students at this school. The offender claimed that he were from Frankfurt, would have conscience (like a murderer) and he also stated to have no concerns about killing. He threatened his chat partner by promising to give him (the chat partner) a headshot with a glock 34 (100 bullets a 9mm).

Background of the dangerous threat: The offender got jealous about a girl, cause he thought that this girl had to much contact with the threatened classmate.

↓

After that incident the service of school psychology immediately contacted the police and in further follow reported the crime at the public prosecutor's office. A "temporary stop" at the proceedings was put forward. A temporary stop signifies that the offender is not going to custody before the judgment (or proceedings) but instead he gets medical treatment. An expert appointed by the court identified, as previously said, a disorder of impulse control with a starting mania and a serious intolerance (the offender freaks out while he is jealous). With close-meshed controlling (a four week interval) and psychiatric medical supervision and appropriate medication it would be possible to put down the danger which is necessary to send somebody in psychiatry.

↓

The prosecution requested an expert report and a supplementary opinion.

↓

The prosecution raised charge under §107 StGB [372] because of threats via Facebook. Note: Actually it is a request for an admission to hospital in accordance with §21 Section 1 StGB [373] as so called predicate offense: Because of mental abnormality, the prosecution applies for an admission to an institution for mentally deranged offenders, whereas the court of lay assessor has decided on this motion.

↓

Finally it was discovered that the offender committed the act of violent threat according to §107 Section 2 StGB, but the judgement pronounced in the sentence that due to a mental abnormality the offender is sent to a psychiatry under the pronounced conditions. The court is regular surveying if the convicted man is meeting the commitments. If he is struggling to commit to those conditions the conditional verdict is revoked and he is going to have immediately a committal to a mental hospital.

[372] §107. (1) Wer einen anderen gefährlich bedroht, um ihn in Furcht und Unruhe zu versetzen, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.
(2) Wer eine gefährliche Drohung begeht, indem er mit dem Tod, mit einer erheblichen Verstümmelung oder einer auffallenden Verunstaltung, mit einer Entführung, mit einer Brandstiftung, mit einer Gefährdung durch Kernenergie, ionisierende Strahlen oder Sprengmittel oder mit der Vernichtung der wirtschaftlichen Existenz oder gesellschaftlichen Stellung droht oder den Bedrohten oder einen anderen, gegen den sich die Gewalt oder gefährliche Drohung richtet, durch diese Mittel längere Zeit hindurch in einen qualvollen Zustand versetzt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

[373] §21. (1) Begeht jemand eine Tat, die mit einer ein Jahr übersteigenden Freiheitsstrafe bedroht ist, und kann er nur deshalb nicht bestraft werden, weil er sie unter dem Einfluß eines die Zurechnungsfähigkeit ausschließenden Zustandes (§11) begangen hat, der auf einer geistigen oder seelischen Abartigkeit von höherem Grad beruht, so hat ihn das Gericht in eine Anstalt für geistig abnorme Rechtsbrecher einzuweisen, wenn nach seiner Person, nach seinem Zustand und nach der Art der Tat zu befürchten ist, daß er sonst unter dem Einfluß seiner geistigen oder seelischen Abartigkeit eine mit Strafe bedrohte Handlung mit schweren Folgen begehen werde.

7.5 Case 5 - Pornographic depiction of minors

A girl aged under 14 incriminated a Serbian adult, that he had coerced her to take nude pictures of herself. He told her that he was going to rush somebody at her if she would not send him nude photos.

↓

It was launched an investigation against this Serbian adult according to §207a (pornographic representation of an underage person) and §105 StGB (coercion) [374]. The investigation regarding §207a was abandoned (§190 (1) StPO [375]), because there were no pornographic images and regarding the coercion §105 StGB criminal applicant was introduced.

↓

The Serbian adult was found not guilty in respect of the coercion because the judge could not find a proof of guilt. Nobody believed into the girl's statement.

↓

Due to that circumstances it was launched an investigation against that girl regarding to pornographic representation, slander and false testimony in front of the court and police. A childish desire to be in the limelight has been recognized, because she took nude pictures on her own and presented them generously to the World Wide Web. Twelve nude images have been subject in this case, eleven of them have just been nude pictures (no pornographic representation) merely one picture fulfilled the fact of pornographic representation.

↓

The girl was quizzed and accused whereupon she refused to testify.

↓

The Prosecutor's office at Innsbruck, suggested to abandon the proceedings regarding §207a StGB (because the fact of pornographic representation was not fulfilled), but the case was sent to the office of the senior public prosecutor and to the ministry of justice for an audit.

[374] §105. (1) Wer einen anderen mit Gewalt oder durch gefährliche Drohung zu einer Handlung, Duldung oder Unterlassung nötigt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Die Tat ist nicht rechtswidrig, wenn die Anwendung der Gewalt oder Drohung als Mittel zu dem angestrebten Zweck nicht den guten Sitten widerstreitet.

[375] §190. Die Staatsanwaltschaft hat von der Verfolgung einer Straftat abzusehen und das Ermittlungsverfahren insoweit einzustellen, als

1. die dem Ermittlungsverfahren zu Grunde liegende Tat nicht mit gerichtlicher Strafe bedroht ist oder sonst die weitere Verfolgung des Beschuldigten aus rechtlichen Gründen unzulässig wäre.

↓

The case was called forward to the office of the senior public prosecutor to judge if the manufacture and distribution of pornographic representation made by the girl fulfills the fact of §207a StGB.

↓

The ministry of justice took the line that those young "actors" can also be culprit of §207a paragraph 1 StGB. This is the case if they share and export those pornographic portrayals. For example teenagers are liable to prosecution if they make accessible lurid, dissorted and reduced to themselves pornographic portrayals via webcam or Email.

↓

The charge regarding §207a Section 1 and 2 StGB was abandoned according to §4 Section 1 JGG because the girl mentioned, that she made the last nude images back in December 2012; it was not lockable if that had really happened before or after her 14th birthday (19 December 1998). If there's any doubt it has to be concluded that she made those images as a minor. It was also not lockable if she shared some of the nude pictures via Facebook in January 2013. The prosecution in Innsbruck appealed to the Supreme Public Prosecutor for the purpose of assessing a not yet sufficiently clarified point of law of fundamental importance, namely the question whether the production or distribution of pornographic material by minors itself satisfies the conditions of §207 Section 1 Clause 1 and 2 StGB. Whilst appealing the Supreme Public Prosecutor, the prosecution in Innsbruck suggested in their report on 18 October 2013 to close proceedings against the minor. The execution in the Federal Ministry of Justice took place on 24 June 2014: According to §207 a StGB an adolescent renders himself/herself to persecution if he/she makes a pornographic depiction of himself/herself accessible to others, even if it is accessible to one person. Lastly, the prosecution in Innsbruck closed proceedings (§207 a StGB) against the minor according to §4 JGG. The allegations of false testimony and slander (to the detriment of the Serbian adult) were done diversionally [376].

[376] Concerning false testimony and slander they agreed on diversion (no previous conviction, it is not shown in the extract from a judicial record and in the reputation) and she has to work in form of community service §201 StPO 30 hours within 3 months at the Association "Neustart". (out-of-court offense resolution)

7.6 Case 6 - Aggravated assault

A person having suffered damages was beaten by a third party and had to be treated in a hospital.

↓

The prosecutor's office opened a criminal proceeding against the defendant for aggravated assault. [377] In this trial, the attorney of the perpetrator has submitted excerpts from medical records of the victim and wanted to demonstrate that the victim had been previous repeatedly beaten and was involved in brawls. These old incidents gathered in medical records are sensitive data and are hence subject of the data protection act 2000. [378]

↓

Due to this fact, the lawyer of the victim became suspicious and wanted to know where the medical record came from. Finally, apart from the fact that medical data is particularly worthy of protection, all identifiable elements of the act, such as name and date of birth, were defaced.

↓

The lawyer of the victim contacted an expert to shed light on this affair and find out, where the sensitive data came from. The expert tried to find out details about the hospital as a note on the medical record prodded him to the xy hospital. The internet research provided promising results, namely the surgical ward.

↓

[377] §84 (1) Hat die Tat eine länger als vierundzwanzig Tage dauernde Gesundheitsschädigung oder Berufsunfähigkeit zur Folge oder ist die Verletzung oder Gesundheitsschädigung an sich schwer, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.
(2) Ebenso ist der Täter zu bestrafen, wenn die Tat begangen worden ist

1. mit einem solchen Mittel und auf solche Weise, womit in der Regel Lebensgefahr verbunden ist,
2. von mindestens drei Personen in verabredeter Verbindung,
3. unter Zufügung besonderer Qualen oder
4. an einem Beamten, Zeugen oder Sachverständigen während oder wegen der Vollziehung seiner Aufgaben oder der Erfüllung seiner Pflichten.

(3) Ebenso ist der Täter zu bestrafen, wenn er mindestens drei selbständige Taten ohne begreiflichen Anlaß und unter Anwendung erheblicher Gewalt begangen hat.

[378] §51. (1) Whoever with the intention to enrich himself or a third person unlawfully or to harm someone in his entitlement guaranteed according to §1 (1) deliberately uses personal data that have been entrusted to or made accessible to him solely because of professional reasons, or that he has acquired illegally, for himself or makes such data available to others or publishes such data with the intention to make a profit or to harm others, despite the data subject's interest in secrecy deserving protection, shall be punished by a court with imprisonment up to a year, unless the offence shall be subject to a more severe punishment pursuant to another provision

The expert communicated this information to the lawyer of the victim, who presented the new facts in the criminal proceeding. The attorney of the opposite site said that he had found this medical act in his mailbox one morning and he did not know where it had come from.

↓

In addition, it turned out that the mother of the defendant was working in the surgical department of the xy hospital and had queried the data from the hospital information system. As far as I know, the perpetrator has been sentenced whereas the mother of the defendant and the perpetrators' attorney were not penalised.

List of Figures

List of Tables

Bibliography

[Ach13] Achim Sawall. Google will keine Third-Party-Cookies mehr zulassen. http://www.golem.de/news/adid-google-will-keine-cookies-mehr-zulassen-1309-101656.html, September 2013. Accessed: 2015-02-17.

[Aig11] Ilse Aigner. Bei Facebook sehe ich viele Fragezeichen. http://www.zeit.de/digital/datenschutz/2011-09/aigner-facebook-datenschutz, September 2011. Accessed: 2015-02-19.

[Alb12] Jan Philipp Albrecht. Datenschutz ist digitaler Umweltschutz: Für eine Reform des europäischen Datenschutzrechts. http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/datenschutz-ist-digitaler-umweltschutz-fuer-eine-reform-des-europaeischen-datenschutzrechts.html, December 2012. Accessed: 2014-12-15.

[Alb13] Jan Philipp Albrecht. General Data Protection Regulation in 10 Points. http://www.janalbrecht.eu/fileadmin/material/Dokumente/131016_Data_protection_press_briefing_final_Engl..pdf, October 2013. Accessed: 2014-09-28.

[Ale12] Alexander Rossnagel, Philipp Richter, Maxi Nebel. Internet Privacy aus rechtswissenschaftlicher Sicht. *Internet Privacy – Eine multidisziplinäre Bestandsaufnahme / A multidisciplinary analysis*, pages 281–327, 2012.

[Art12] CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=DE, October 2012. Accessed: 2014-12-15.

[Ber09] Nicole Bergmann. *Volkszählung und Datenschutz - Proteste zur Volkszählung 1983 und 1987 in der Bundesrepublik Deutschland.* Diplomica Verlag GmbH, 2009.

[Bun] Bundeskanzleramt. OECD - Organisation für wirtschaftliche Zusammenarbeit und Entwicklung. http://www.bundeskanzleramt.at/DesktopDefault.aspx?TabID=3469&Alias=BKA. Accessed: 2015-01-15.

[Bun08] Bundeskanzleramt. Entwurf Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008). http://www.parlament.gv.at/PAKT/VHG/XXIII/ME/ME_00182/fnameorig_106408.html, 2008. Accessed: 2014-11-11.

[Bun09] Bundeskanzleramt. Entwurf Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010). http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062/fnameorig_158877.html, 2009. Accessed: 2014-11-11.

[Bun10a] Bundeskanzleramt. Artikel 8 - Recht auf Achtung des Privat- und Familienlebens. https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12016939, August 2010. Accessed: 2014-11-25.

[Bun10b] Bundeskanzleramt. Bildnisschutz. https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12024485, March 2010. Accessed: 2014-11-25.

[Bun10c] Bundeskanzleramt Österreich. Google-Street-View: Stellungnahme und Forderungen des Datenschutzrates. http://www.bka.gv.at/site/cob__39694/6343/default.aspx, May 2010. Accessed: 2015-02-06.

[Cha00] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION. http://www.europarl.europa.eu/charter/pdf/text_en.pdf, December 2000. Accessed: 2014-08-26.

[Chr14] Christian Lenoble. Big Data – Chancen, Gefahren, Grenzen. *WU Magazin Informationen aus der Wirtschaftsuniversität Wien*, 3:3–6, 2014.

[CJL13] Julia M. Siripurapu Cynthia J. Larose. Guide to Compliance with the Amended COPPA Rule. http://www.mintz.com/newsletter/2013/Advisories/3183-0613-NAT-PRIV/index.html, June 2013. Accessed: 2014-02-17.

[COD03] ORGANISATION FOR ECONOMIC CO-OPERATION and DEVELOPMENT. Overview - OECD-Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (German translation). http://www.oecd.org/sti/ieconomy/15589558.pdf, 2003. Accessed: 2015-01-22.

[Com07] Federal Trade Commission. Implementing the Children's Online Privac Protection Act - A Report to Congress. http://www.ftc.gov/sites/default/files/documents/reports/implementing-childrens-online-privacy-protection-act-federal-trade-commission-report-congress/07coppa_report_to_congress.pdf, February 2007. Accessed: 2014-02-17.

[Com10] Data protection in the electronic communications sector. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1414502275988&uri=URISERV:l24120, May 2010. Accessed: 2014-10-17.

[Cou14] Court of Justice of the European Union. The Court of Justice declares the Data Retention Directive to be invalid. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, April 2014. Accessed: 2014-10-23.

[Dan09] Daniele Catteddu, Giles Hogben. Cloud Computing: Benefits, risks and recommendations for information security. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport, November 2009. Accessed: 2015-02-20.

[Der13] Christoph Dernbach. Anleitung: Twitter für Einsteiger – Tipps und Tricks für den Microblogging-Dienst (1). http://www.mr-gadget.de/howto/2013-03-21/twitter-fuer-einsteiger-tipps-und-tricks-fuer-den-microblogging-dienst-1, March 2013. Accessed: 2015-01-31.

[Dir95] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of indidivuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=de, November 1995. Accessed: 2014-10-18.

[Dir02] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=DE, July 2002. Accessed: 2014-08-23.

[Dir06] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, April 2006. Accessed: 2014-10-06.

[Dom13] Dominik Klein, Phuoc Tran–Gia, Matthias Hartmann. Big Data. *Informatik Spektrum*, pages 319–323, 2013. Springer Verlag Berlin Heidelberg.

[Dr.14] Dr. Rainer Knyrim, Dr. Gerald Trieb LL.M. Smart Metering – neue Vorgaben aus Europa durch das künftige Datenschutzrecht. *Oesterreichs Energie – Fachmagazin der österreichischen E-Wirtschaft*, pages 54–57, June 2014.

[Dr.15] Dr. Thomas Helbing. Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung. *Kommunikation & Recht: Betriebs-Berater für Medien, Telekommunikation, Multimedia*, pages 145 – 150, March 2015.

[DRK14] Dr. Gerald Trieb LL.M. Dr. Rainer Knyrim. Das künftige EU-Datenschutzrecht – Neue Anforderungen an die unternehmerische Compliance. *Compliance Praxis*, pages 30–33, February 2014.

[DSG78] Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG), BGBI 1978/565. https://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf, November 1978. Accessed: 2014-10-17.

[DSG14] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DS1978/565 BGBI 1999/165. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597, July 2014. Accessed: 2014-10-02.

[Dus09] Alfred Duschanek. *Handbuch Datenschutzrecht 2009 - Videoüberwachung, E-Government, Arbeitsrecht, Steuerrecht, Unternehmenskauf, Sicherheitspolizei*, chapter Die Entwicklung des Datenschutzes in Österreich, pages 43–46. Facultas Verlags- und Buchhandels AG, 2009.

[Eck15] Peter Eckersley. Which Apps Protect Against Verizon and Turn's Invasive User Tracking? https://www.eff.org/de/deeplinks/2015/01/which-apps-and-browsers-protect-you-against-verizon-and-turns-non-consensual, January 2015. Accessed: 2015-02-08.

[ELG06] ARGE ELGA. Machbarkeitsstudie bezüglich Einführung der elektronischen Gesundheitsakte (ELGA) im österreichischen Gesundheitswesen. Technical report, IBM im Auftrag der Bundesgesundheitsagentur, 2006.

[fdDufdRaAB] Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg. Geschichte des Datenschutzes. `http://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.251507.de`. Accessed: 2014-09-24.

[fM09a] Ludwig Boltzmann Institut für Menschenrechte. BIM-Entwurf zur TKG-Novelle 2010. `http://bim.lbg.ac.at/sites/files/bim/BIM-Entwurf%20TKG-Novelle%202010.pdf`, September 2009. p. 1–13, Accessed: 2014-10-03.

[fM09b] Ludwig Boltzmann Institut für Menschenrechte. BIM-Entwurf zur Vorratsdatenspeicherung in Begutachtung. `http://bim.lbg.ac.at/de/informationsgesellschaft/bimentwurf-zur-vorratsdatenspeicherung-begutachtung`, November 2009. Accessed: 2014-10-01.

[Gen04a] Alexander Gentz. *Datenschutz in Europa und den USA: eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung*. DuD-Fachbeiträge. Dt. Univ.-Verl. Wiesbaden, 2004.

[Gen04b] Alexander Genz. *Datenschutz in Europa und den USA - Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung*. Andreas Pfitzmann, Helmut Reimer, Karl Rihaczek und Alexander Roßnagel, 2004.

[Gen12] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). `http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf`, January 2012. Accessed: 2014-10-15.

[Ger09] Ben Gerber. OECD Privacy Principles. `http://oecdprivacy.org/`collection, 2009. Accessed: 2015-01-22.

[Gra10] Wolfgang Graf. *Datenschutzrecht im Überblick*. Facultas Verlags- und Buchhandels AG, 2010.

[Han14] Hannes Grassegger. Jeder hat seinen Preis: Unendlich viele Preise für ein Produkt: Einer der größten kapitalistischen Träume ist gerade dabei, in Erfüllung zu gehen. Big Data macht es möglich. `http://www.zeit.de/wirtschaft/2014-10/absolute-preisdiskriminierung`, October 2014. Accessed: 2015-02-10.

[Hes12] Hessisches Landesamt für geschichtliche Landeskunde. Hessischer Landtag verabschiedet das weltweit erste Datenschutzgesetz, 7. Oktober 1970 in Zeitgeschichte in Hessen. http://lagis.online.uni-marburg.de/de/subjects/idrec/sn/edb/id/204, June 2012. Accessed: 2014-09-25.

[Hil14] Felix Hilgert. Datenschutz in den USA: Ist COPPA ein Kinderspiel? http://spielerecht.de/datenschutz-in-den-usa-ist-coppa-ein-kinderspiel/, August 2014. Accessed: 2014-02-17.

[Hol02] Heike Holzhausen. Die Safe-Harbor-Vereinbarung als Methode zur Sicherung eines "angemessenen Datenschutzniveaus" im Sinne der EG-Datenschutzrichtlinie. http://eulisp.org/tl_files/eulisp%20abschlussarbeiten/holzhausen_heike.pdf, January 2002. Accessed: 2015-01-20.

[Iaf14] Fernando Iafrate. *Digital Enterprise Design & Management*, chapter A Journey from Big Data to Smart Data, pages 25–30. Springer International Publishing Switzerland, 2014.

[Int13] International Working Group on Data Protection in Telecommunications. Arbeitspapier Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar. www.datenschutz-berlin.de/attachments/951/675.46.18.pdf, April 2013. Accessed: 2015-02-10.

[Jam14] Josh James. Data Never Sleeps 2.0. http://www.domo.com/blog/2014/04/data-never-sleeps-2-0/, April 2014. Accessed: 2014-12-09.

[Jas10] Jasper von Altenbockum. Die Richtlinie, nach der sich nicht alle richten. http://www.faz.net/aktuell/politik/europaeische-union/vorratsdatenspeicherung-die-richtlinie-nach-der-sich-nicht-alle-richten-1953395.html, March 2010. Accessed: 2014-10-17.

[Joc] Jochen Schneider. Fokus und Raster des Datenschutzes im nichtöffentlichen Bereich: Hinterfragung und Erneuerung. http://edoc.hu-berlin.de/miscellanies/steinmueller-40657/225/PDF/225.pdf. Accessed: 2014-10-17.

[Joh12] Johannes Buchmann. Internet Privacy - Eine multidisziplinäre Bestandsaufnahme / A multidisciplinary analysis. Technical report, acatech - Deutsche Akademie der Technikwissenschaften, 2012. Springer Verlag.

[Kar13] Internet Safety Project Karianne. Please rob me. https://www.internetsafetyproject.org/wiki/please-rob-me, 2013. Accessed: 2015-01-31.

[Kno10] Mag. Martin Knoll. Zur datenschutzrechtlichen (Un)Zulässigkeit von Google Street View. *jusIT*, 1:16–19, 2010.

[Kny10] Knyrim. Die neue "Data Breach Notification Duty" im DSG. *Datenschutzrecht Jahrbuch*, 2010.

[Kny12a] Dr. Rainer Knyrim. Draft of the EU General Data Protection Regulation. http://www.preslmayr.at/tl_files/Publikationen/2014/Entwurf%20der%20neuen%20EU-Datenschutz-Grundverordnung_Knyrim.pdf, May 2012. p. 25–38, Accessed: 2014-10-02.

[Kny12b] Rainer Knyrim. *Datenschutzrecht - Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm.* Manz'sche Verlags- und Universitätsbuchhandlung GmbH, 2012.

[Kot13] David Kotrba. Drohnen im zivilen Luftraum: "Nicht so einfach". http://futurezone.at/digital-life/drohnen-im-zivilen-luftraum-nicht-so-einfach/24.600.547, August 2013. Accessed: 2015-02-02.

[Kro15] Oona Kroisleitner. "Sexting": Zwischen Flirten und Bloßstellung. http://derstandard.at/2000011341821/Sexting-Zwischen-Flirten-und-Blossstellung, February 2015. Accessed: 2015-02-11.

[Kus10] Dan Kusnetzky. What is "Big Data?". http://www.zdnet.com/blog/virtualization/what-is-big-data/1708 (Archived by WebCiteÂő at http://www.webcitation.org/6DkS9jaPP), February 2010. Accessed: 2014-12-09.

[Lec09] Georg Lechner. *Handbuch Datenschutzrecht 2009 - Videoüberwachung, E-Government, Arbeitsrecht, Steuerrecht, Unternehmenskauf, Sicherheitspolizei*, chapter Datenschutz und Internet, pages 209–231. Facultas Verlags- und Buchhandels AG, 2009.

[Lec11] Rachid Lechheb. Forthehack - PleaseRobme - Audio Visual Presentation. http://vimeo.com/10892460, 2011. Accessed: 2015-01-31.

[LS14] Sabine Leutheusser-Schnarrenberger. Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa. *Datenschutz und Datensicherheit - DuD*, 38:589–592, September 2014.

[Lud08] Ludwig Boltzmann Institut für Menschenrechte (BIM) in Kooperation mit dem Institut für Rechtsinformatik der Leibniz Universität Hannover (IRI). Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung. http://bim.lbg.ac.at/files/sites/bim/Rechtsvergleich_Vorratsdatenspeicherung.pdf, March 2008. Accessed: 2014-10-17.

[Luf13] Bundesgesetz vom 2. Dezember 1957 über die Luftfahrt (Luftfahrtgesetz – LFG). BGBl. I Nr. 108/2013 (NR: GP XXIV RV 2299 AB 2349 S. 203. BR: AB 8984 S. 821.). https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10011306, 2013. Accessed: 2015-02-05.

[Lui] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, Maik Lindner. A Break in the Clouds: Towards a Cloud Definition.

[Mag11a] Mag. Alexander Ströher, Mag. Wilfried Honekamp. ELGA – die elektronische Gesundheitsakte vor dem Hintergrund von Datenschutz und Datensicherheit. *Wiener Medizinische Wochenschrift*, pages 341–346, June 2011.

[Mag11b] Mag. Karin Peyerl. Cloud Computing – Datenschutzrecht Aspekte bei der "Datenverarbeitung in der Wolke". *jusIT*, pages 57–64, February 2011.

[Mar12] Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri. *Einführung in das Datenschutzrecht - Datenschutz und Informationsfreiheit in europäischer Sicht*. Oldenburg Verlag, 5. vollständig überarbeitete auflage edition, 2012. p. 415–417.

[Mar13] Martin Pscheidl. Data Breach Notification - Österr. Informationspflicht bei Datenlecks. http://www.externerdatenschutzbeauftragter.at/data-breach-notification/, May 2013. Accessed: 2014-10-17.

[Mar14a] Mark van Rijmenam. Why The 3Vs Are Not Sufficient To Describe Big Data. https://datafloq.com/read/3vs-sufficient-describe-big-data/166, August 2014. Accessed: 2015-01-01.

[Mar14b] Markus Schneider, Matthias Enzmann, Martin Stopczynski. Web-Tracking-Report 2014. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf, February 2014. Accessed: 2015-02-06.

[Mat14a] Matthew L. Bycer. Understanding the 1890 Warren and Brandeis "The Right to Privacy" Article. `http://juris.nationalparalegal.edu/%28X%281%29S%28ocz4hwbtqp2wdrw2r3z2oapg%29%29/UnderstandingWarrenBrandeis.aspx`, 2014. Accessed: 2015-02-20.

[Mat14b] Matthias Orthwein, Katrin Anna Rücker. Kann Europa von Kalifornien Datenschutz lernen? Data Breach, Do Not Track und das Recht auf Vergessen im Gesetzgebungsvergleich. *Datenschutz und Datensicherheit – DuD*, 38:613–618, September 2014.

[Mey15] Jonathan Meyer. The Turn-Verizon Zombie Cookie. `http://webpolicy.org/2015/01/14/turn-verizon-zombie-cookie/`, January 2015. Accessed: 2015-02-08.

[Mil13] Miller, H.E. Big-data in cloud computing: A taxonomy of risks. *Information Research, 18(1) paper 571*, 2013. Available at `http://InformationR.net/ir/18-1/paper571.html`.

[Min14] Min Chen, Shiwen Mao, Yin Zhang, Victor C.M. Leung. *Big Data - Related Technologies, Challenges and Future Prospects*. Springer Verlag, 2014.

[MSC13] Viktor Mayer-Schönberger and Kenneth Cukier. *Big Data A Revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt Publishing Company, 2013.

[Mül08] Klaus-Rainer Müller. *IT-Sicherheit mit System.* Vieweg Verlag, 3. erweiterte und aktualisierte auflage edition, 2008.

[Mül10] Klaus-Rainer Müller. *Handbuch Unternehmenssicherheit - umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System.* Vieweg + Teuber Verlag, 2 edition, 2010.

[Neu14] Benedikt Neuroth. *Narrative Formen der Politik*, chapter "The Specter of Orwell": Narrative nach Nineteen-Eiighty-Four in US-amerikanischen Privacy-Debaten der 1960er und 1970er Jahre, pages 73–90. Springer Fachmedien Wiesbaden, 2014.

[N.Na] N.N. Article 8 ECHR. `http://echr-online.info/article-8-echr/`. Accessed: 2015-04-17.

[N.Nb] N.N. Neue Entwicklungen betreffend Google Street View. `http://www.dsb.gv.at/site/6733/default.aspx`. Accessed: 2015-02-06.

[N.N09] N.N. Forthehack. `http://www.forthehack.com/`, 2009. Accessed: 2015-01-31.

[N.N11a] N.N. Datenschutzkommission: "Google Street View ist in Österreich zulässig". http://derstandard.at/1303291129391/Datenschutzkommission-Google-Street-View-ist-in-Oesterreich-zulaessig, April 2011. Accessed: 2015-02-05.

[N.N11b] N.N. Grünes Licht für Google Street View in Österreich. http://futurezone.at/netzpolitik/gruenes-licht-fuer-google-street-view-in-oesterreich/24.565.627, April 2011. Accessed: 2015-02-05.

[N.N12a] N.N. Google Street View in Österreich: Zumindest auf Skipisten. http://derstandard.at/1353207542963/Google-Street-View-in-Oesterreich-Zumindest-auf-Skipisten, November 2012. Accessed: 2015-02-07.

[N.N12b] N.N. Sexting. https://www.onlinesicherheit.gv.at/kinder_und_jugendliche/belaestigung_und_cyber_mobbing/sexting/73166.html, October 2012. Accessed: 2015-02-11.

[N.N13a] N.N. Bures lässt Drohnen nicht mehr frei herumfliegen - Ein neues Luftfahrtgesetz regelt Filmaufnahmen für Gewerbezwecke und Aktivitäten von Hobbyfliegern. http://diepresse.com/home/techscience/hightech/1393589/Bures-laesst-Drohnen-nicht-mehr-frei-herumfliegen, April 2013. Accessed: 2015-02-05.

[N.N13b] N.N. Drohnen-Gesetz soll Privatgebrauch einschränken. http://futurezone.at/netzpolitik/drohnen-gesetz-soll-privatgebrauch-einschraenken/24.595.602, April 2013. Accessed: 2015-02-05.

[N.N14a] N.N. Cookies und Webtracking - Vor den Datensammlern der Werbewirtschaft schützen. https://www.saferinternet.at/news/news-detail/article/cookies-und-webtracking-vor-den-datensammlern-der-werbewirtschaft-schuetzen-440/, July 2014. Accessed: 2015-02-10.

[N.N14b] N.N. Extract: Decision G 47/2012 e.a. regarding data retention. https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/erwaegungeneng28082014.pdf, June 2014. Accessed: 2015-04-17.

[N.N14c] N.N. Kein Google Street View für Österreich. http://www.kleinezeitung.at/s/lebensart/multimedia/4180750/Datenschutz_Kein-Google-Street-View-fur-Osterreich, August 2014. Accessed: 2015-02-06.

[N.N14d] N.N. Press Release - Austrian Laws on Data Retention Found Unconstitutional. https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/press_releasedataretention.pdf, June 2014. Accessed: 2015-04-17.

[N.N14e] N.N. Privacy Policy - Full Privacy Policy. https://www.verizon.com/about/privacy/policy/, August 2014. Accessed: 2015-02-08.

[N.N14f] N.N. So sammeln Unternehmen User-Daten. http://www.ksta.de/fraunhofer/sote-web-tracking--so-sammeln-unternehmen-user-daten,26145496,26738832.html, July 2014. Accessed: 2015-02-20.

[N.N14g] N.N. Stadion der Austria Wien jetzt in Street View verfügbar. http://derstandard.at/2000004052948/Stadion-der-Austria-Wien-jetzt-in-Street-View-verfuegbar, August 2014. Accessed: 2015-02-07.

[N.N15a] N.N. Aktuelle Studie: Sexting in der Lebenswelt von Jugendlichen. http://www.saferinternet.at/news/news-detail/article/aktuelle-studie-sexting-in-der-lebenswelt-von-jugendlichen-489/, February 2015. Accessed: 2015-02-11.

[N.N15b] N.N. Aktuelle Studie: Versand von eigenen Nacktaufnahmen unter Jugendlichen nimmt zu. 3.http://www.ots.at/presseaussendung/OTS_20150205_OTS0110/aktuelle-studie-versand-von-eigenen-nacktaufnahmen-unter-jugendlichen-nimmt-zu-bild, February 2015. Accessed: 2015-02-11.

[N.N15c] N.N. Foursquare. https://de.foursquare.com/, 2015. Accessed: 2015-01-31.

[N.N15d] N.N. Häufige Fragen und Antworten zu Sexting. http://www.saferinternet.at/fileadmin/files/Sexting_Studie/FAQ_Sexting.pdf, February 2015. Accessed: 2015-02-11.

[Nor13] Kevin Normandeau. Beyond Volume, Variety and Velocity is the Issue of Big Data Veracity. http://insidebigdata.com/2013/09/12/beyond-volume-variety-velocity-issue-big-data-veracity/, September 2013. Accessed: 2015-01-01.

[OEC60] OECD. Übereinkommen über die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung. http://www.oecd.org/berlin/dieoecd/ubereinkommenuberdieorganisationfurwirtschaftlichezusammenarbeitundentwicklung.htm, December 1960. Accessed: 2015-01-22.

[oJA01] Council of Justice and Home Affairs. Ratsdok. SN 3926/6/01 REV 6, Conclusions adopted by the Council (Justice and Home Affairs), Schlussfolgerung Nr. 4, Brüssel, September 2001.

[oJA02] Council of Justice and Home Affairs. Ratsdok. 15691/02, 2477th Council meeting (Justice and Home Affairs), Schlussfolgerung Nr. 5 des Kapitels Informationstechnologien und die Aufklärung sowie Ahndung organisierter Kriminalität, Brüssel, December 2002.

[Pas15] Pascal Schneiders. Jeder kriegt seinen eigenen Preis. `http://www.faz.net/aktuell/finanzen/meine-finanzen/geld-ausgeben/dynamische-preise-das-ende-des-einheitspreises-13522679.html`, April 2015. Accessed: 2014-10-17.

[Pat10] Frank Patalong. PleaseRobMe: Mein Auto, mein Haus, meine Yacht (ist weg!). `http://www.spiegel.de/netzwelt/web/pleaserobme-mein-auto-mein-haus-meine-yacht-ist-weg-a-678934.html`, February 2010. Accessed: 2015-01-31.

[PM11] Timothy Grance Peter Mell. The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. `http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf`, September 2011. Accessed: 2014-11-25.

[RA 12] RA Dr. Michael M. Pachinger. Der neue "Cookie-Paragraph" – Erste Gedanken zur Umsetzung des Art 5 E-Privacy-RL in §96 Abs 3 TKG 2003 idF BGBI I 2011/102. *jusIT*, (1), 2012.

[RA 14] RA Dr. Michael M. Pachinger. Neue Leitlinien für die Cookie-Einwilligung. *jusIT*, (2), 2014.

[Rai10] Rainer Knyrim, Günther Leissler. Die Datenschutzgesetznovelle 2010 - ein Überblick. *ecolex*, 2010.

[Rai11] Rainer Knyrim, Viktoria Haidinger. Cloud Computing – trübe Aussichten für ein neues Geschäftsmodell. *ecolex*, pages 562–565, 2011.

[Rat04] Ratsdok. 8958/04, Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, April 2004.

[Rig] Context - The right to privacy. `http://faculty.uml.edu/sgallagher/harvard__law_review.htm`. Accessed: 2014-09-23.

[Rob14] Robert Rothmann. Videoüberwachung und Auskunftsrecht. *Datenschutz und Datensicherheit - DuD*, pages 405–406, May 2014.

[Rol08] Roland Steidle, Ulrich Pordesch. Im Netz von Google. Web-Tracking und Datenschutz. *Datenschutz und Datensicherheit - DuD*, 32:324–329, 2008.

[Rös] Beate Rössler. Der Wert des Privaten. https://www.dpunkt.de/leseproben/1888/Kapitel%201.pdf. Accessed: 2014-09-23.

[Rös01] Beate Rössler. *Der Wert des Privaten.* Suhrkamp Verlag, 2001.

[Saf] U.S.-EU SAFE HARBOR LIST. https://safeharbor.export.gov/list.aspx. Accessed: 2014-01-11.

[Sam90] Samuel D. Warren and Louis D. Brandeis. Harvard Law Review Vol. IV No. 5 - The Right to Privacy. http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm, 12 1890. Accessed: 2014-09-23.

[Seb13] Sebastian Hofer. Zahlenmäßig überlegen: "Big Data". http://www.profil.at/home/zahlenmaessig-big-data-354256, March 2013. Accessed: 2015-02-20.

[Sic13] Svetlana Sicular. Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s. http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/, March 2013. Retrieved 09 December 2014.

[Sim96] Simone Fischer-Hübner, Kathrin Schier. Der Weg in die Informationsgesellschaft - Eine Gefahr für den Datenschutz. *Schnittstellen Theorie der Informatik*, 1996.

[SK13] Eva Souhrada-Kirchmayer. *Datenschutzrecht und E-Government. Jahrbuch 2013.* Dietmar Jahnel, 2013.

[Sol14] Christian Solmecke. Die rechtlichen Probleme des Einsatzes von zivilen Drohnen. https://www.wbs-law.de/internetrecht/die-rechtlichen-probleme-des-einsatzes-von-zivilen-drohnen-49854/, January 2014. Accessed: 2015-02-05.

[Son10] Michael Sonntag. *Einführung in das Internetrecht - Rechtsgrundlagen für Informatiker.* Linde Verlag, 2010.

[Ste15] Martin Stepanek. Sexting: Jeder dritte Jugendliche erhält Nacktfotos. http://futurezone.at/digital-life/sexting-jeder-dritte-jugendliche-erhaelt-nacktfotos/112.119.455, February 2015. Accessed: 2015-02-03.

[Tho15] Jörg Thoma. US-Vermarkter nutzt Zombie-Cookies. http://www.golem.de/news/tracking-us-vermarkter-nutzt-zombie-cookies-1501-111721.html, January 2015. Accessed: 2015-02-08.

[Tre07] Official Journal of the European Union - Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. `http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=EN`, December 2007. p.15, Accessed: 2014-08-30.

[Vik14] Viktor Mayer-Schönberger, Ernst Brandl, Hans Kristoferitsch. *Datenschutzgesetz - Grundsätze und europarecheuropa Rahmenbedingungen, Gesetztestext mit Materialien, Datenschutz-Verordnungen und Richtlinien im Anhang.* Linde Verlag, 2014. 3. aktualisierte Auflage.

[Wes09] Dietrich Westphal. *Handbuch Datenschutzrecht 2009 - Videoüberwachung, E-Government, Arbeitsrecht, Steuerrecht, Unternehmenskauf, Sicherheitspolizei*, chapter Grundlagen und Bausteine des europäischen Datenschutzrechts, pages 53–94. Facultas Verlags- und Buchhandels AG, 2009.