MASTERARBEIT

Titel der Masterarbeit

“The European data protection laws
and their practical application in Austria and Sweden”

Verfasser

BSc Robert Hoffmann

angestrebter akademischer Grad

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2011

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienblatt:	Wirtschaftsinformatik
Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Contents

Chapter 1
Introduction

1.1 Motivation and background

The European Union strives to unify its data and privacy protection laws to simplify business and legal questions across its member states. But since every country has to implement them by creating specific local laws their respective adaptions differ.

Large, multi-national companies are usually aware of this situation and are capable to adapt accordingly. They utilize their own legal department or consultants and a tightly organized, process orientated IT environment for this.

Smaller and medium-sized businesses (SMBs), who span usually just one or two countries and barely have a basic IT department, often lack this kind of organization. In the worst case they are not aware of the legal implications of their IT environment and don't protect their business data accordingly. Usually this stems from a lack of legal knowledge and a low awareness of the EU regulations within those IT departments. Typically they do have a sound knowledge of their applicable business regulations, but consider their IT infrastructure to be some kind of evolved typewriter. Information and data is handled in the same way as it was until now on paper, with no considerations to the new threats which arose from digitalization.

It can be observed that the origin of this problem mostly is a

1. lack of time for duties which do not have a direct effect on the daily business
2. lack of knowledge in business informatics

The first issue results from the fact that those small IT groups are direct subordinates of their business leaders. Therefore exists a high incentive for the business to avoid any work which doesn't result in a short-term profit or advantage.

This goes hand in hand with the second issue, which exists because the business leaders and the IT staff usually don't have any education in the field of business informatics. The business knows that it has to stream-line its processes and the IT staff knows how to work with hard- and software, but they lack the understanding of each others domain and therefore can't utilize their IT in the most effective way. Since the IT department is subordinated to the business this often results in technically questionable or even dangerous solutions.

1.2 Goal of this document

To improve the situation in a SMB this document aims to provide small IT departments with all the basic knowledge on how to comply with the various data and privacy protection laws.

A sound knowledge of current legal issues will be provided, together with the applicable laws on a European and national level.

The IT department should receive all necessary information and tools to implement a useful information security process and protect its assets according to their value and the applicable law. Checklists and other documents should serve as templates for a quick and easy application of this knowledge in the daily work.

Since a core area of any business is to communicate, close attention will be paid to the areas of homepages, e-commerce and emails.

This work should serve as a information resource for business IT departments. It will therefore look at the consumers rights and data protection requirements from the viewpoint of the business and how it is required to protect the data of its customers.

Apart from the legal perspective, one also needs to consider the organizational and technical structure. Therefore a guideline about how to structure the IT department and some basic philosophy behind data handling will be provided. The aim is to provide an understanding about the differences between technical data handling and organizational information work in regard to legal issues.

1.3 Structure of this document

After chapter one, the introduction, in chapter two an overview over the current legal situation in the EU is given. It will show the intentions of the EU directives and how this affects consumers and other market participants. Although those directives don't apply directly, it is the basis for the national laws and regulations.

The third and forth chapters show in detail how the EU directives are applied in local legislation in Austria and Sweden and how this affects a local

SMB. Also national court decisions will be investigated to discuss how the national courts apply the EU requirements.

In chapter five both countries are compared to each other. It starts with a general comparison of how they approach the EU legislations and then show the differences that a business will face if it operates in both of them.

The sixth chapter provides guidelines and tools for a small IT department to apply the national laws and regulations. Differences between Austria and Sweden and their effects on the IT operation will be discussed, if they exist.

Chapter six will also show that the terms “data” and “information” are actually used in a wrong sense in the legal context, as seen from a scientific viewpoint. But to stay within the same terminology and allow for easier reading of the legal texts, the correct terms are not utilized in the chapters before it.

A summary and final conclusion is given in chapter seven and eight.

The appendix provides templates for the IT department to apply this knowledge in their daily work.

At the end of the document an abstract in English and German is give, together with the CV of the author.

1.4 Methodology

Chapter two about the EU regulations will be a qualitative research, to define the area of data protection and how the EU sees it. This is done by investigating all relevant directives and how they define various terms.

Chapter three and four about Austria and Sweden are a combination of qualitative and quantitative methods. First the local law and its terms will be looked at, similar to chapter two. Then a selection of local court decisions will be shown and evaluated in regard to their relevance to a business environment.

A comparative analysis is done in chapter five to show differences between the two countries.

Chapter six provides definitions according to Zins’ DIKW model [173] and then uses a deductive approach to provide data handling processes that are in accordance with the EU directives.

Chapter 2
EU laws and regulations

2.1 Overview

Before the EU treaty each European country had its own, different, or even none legislation regarding information handling and commerce utilizing IT systems. The EU recognized [8, § 0] that a common, unified legislation will support and push forward business activities and therefore economic wealth between the countries - if, and this has also been recognized as a main issue, the market participants trust in the security and privacy of the involved data.

This trust is also a main concern within organizations. It is required that employees trust their employer and citizens trust their government that the private data they supply is well protected and laws are in place to enforce this protection.

Otherwise any party will be very reluctant to give away any data, and public or economic information exchange will receive a severe negative impact.

The EU has identified several core areas and created according regulations. From the timeline and the naming of those one can easily see, that the main goal is to provide a basis for commercial collaboration. This should also be the main concern for any business - the trust of the other party is required to receive their data.

It is worth noting that most of the regulations apply to commercial businesses and government agencies in the same way, which means that the EU usually does not want to separate between private and state owned parties.

The EU directives also require an organized IT department with clearly defined responsibilities. Otherwise it will not be possible to implement effective access rights schemes or provide useful logging and monitoring.

Although most of the mentioned services and techniques have their origin in the Internet, the directives are written to be technology neutral, they generally apply to any transaction that takes place between two parties who are not in the same place, but communicate by utilizing some technical means.

2.1.1 Commerce using electronic communication

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") [8]

2.1.2 Protection of consumers

- Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts [5]
- Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC [19]

2.1.3 Digital signatures

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [7]

2.1.4 Electronic money

- Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions [10]

2.1.5 Intellectual property

- Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs [2]
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [4]

- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society [11]

2.1.6 Internet domain names

- Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain [20]

2.1.7 Data privacy and protection

- 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) [18]
- Directive 95/46/EC of the European Parliament and of 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 [3]
- 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [12]
- 2002/16/EC: Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries , under Directive 95/46/EC [13]
- 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [23]

2.1.8 Jurisdiction in international electronic transactions

- 1980 Rome Convention on the law applicable to contractual obligations [1]
- Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [9]
- Commission Regulation (EC) No 1496/2002 of 21 August 2002 amending Annex I (the rules of jurisdiction referred to in Article 3(2) and Article

4(2)) and Annex II (the list of competent courts and authorities) to Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [21]
- Commission Regulation (EC) No 2245/2004 of 27 December 2004 amending Annexes I, II, III and IV to Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [24]

2.1.9 Electronic communications networks

- Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) [14]
- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) [15]
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [16]
- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) [17]

2.1.10 Surveillance and access protection

- Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access [6]
- 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 [25]

2.2 Data protection

2.2.1 Definitions

The legal binding definitions can be found in the EU directive [3, art. 2], and a short summery is provided here:

2.2.1.1 Personal data

> "Personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; [18, art. 2a]

This means that any data that relates to a person or any data by which a person can be identified, has to be considered. There is no distinction made if this data is considered "valuable" (to whomever) or if this information is already available to the public. As one can see, this covers a lot of data in common business IT systems. It is also important to point out that any kind of information could be "personal data" - not only data records, but also audio and video files, paper or other media. The core concept here is the relation of the data to a certain person.

There is also no distinction being made about how this data was received, it may be by electronic means, on paper, by voice or otherwise.

2.2.1.2 Sensitivity

A further distinction is being made regarding the sensitivity of the data:

1. sensitive data [3, art. 8 lit. 1]

   a. racial or ethnic origin
   b. political opinions
   c. religious or philosophical beliefs
   d. trade-union membership
   e. data concerning health or sex life

2. personal data

   a. any other data which can be related to a person

Biometric data, like fingerprints or weight, is considered personal data, except if it indicates any information about health; this has to be taken into account when designing biometric access controls. This area also has to be reevaluated from time to time, as new discoveries in science might allow to extract sensitive information from former harmless biometric data, for example it might be possible in the future to identify certain medical conditions from the the fingerprint of a person.

2.2.1.3 Handling

It is important to distinguish between two activities:

- Processing
- Transfer

Processing can be done by the company itself or a subcontractor, who of course needs access to this data. If he doesn't have direct access, but instead receives a copy of the data then this is still covered by the term "processing". If the subcontractor is not located in the EU or other accredited countries (having the same level of legal data protection) then the approval of the local legal entity is required.

Transfer on the other hand regards the sending of a copy to another entity, for their own purpose (assuming, of course, that the transfer is approved by the data owner). Again, no distinction is being made about how the transfer is done or which medium is used for this. Sending an electronic record, giving the information by phone or publishing it on paper has the same relevance.

Any handling of data inside a company is not considered a transfer, as long as it stays within one logical unit. The underlying organizational structure has no influence here, the important fact is the logical structure. It is therefore mandatory that the company has a clean structure with clearly defined responsibilities and processes.

This on the other hand also means that the transfer of personal data from one business unit to another is only legitimate if the data owner has been made aware of it and has approved it. For example a larger finance corporation can not use its customer data from the insurance business unit for marketing purposes of its banking unit.

A special case is a company supported club, for example a sports club organized by the employees, who utilizes the IT infrastructure of the company. This usually takes the form of an internal homepage and emails to its members. In this case the separate legal entity of the club uses the company as a subcontractor, therefore the club is responsible for the protection of the personal data.

2.2.1.4 Storage

The EU legislation considers only certain kinds of data storage, although this usually will cover most of the existing databases:

> Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question. [3, § 0 art. 15]

Unsorted, chaotic collections of personal data are therefore not covered.

Furthermore the directive states “criteria”, which is also translated as a plural in other languages. It has therefore been deducted, e.g. in Sweden, that only databases which can be searched by two or more criteria are covered. Collections that are only accessible through one kind of search term, e.g. a telephone book that is sorted only by name, are therefore not protected.

It is also worth noting that there is no mentioning of the storage media; it does not matter if the data is put on paper, audio or electronic storage devices, it also does not matter if the data will be processed automatically or manually.

2.2.2 Data protection philosophy

The main idea in the EU is that data shall only be collected for a certain purpose and with the consent of the data owner:

> Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified [3, § 0 art. 28]

One of the core principles of the EU legislation is that any personal data is always owned by that person and that this owner can’t give away those rights. Instead he can only allow others to process or use this data. This means for example, that if a photograph is taken of an employee and put on his company ID card, he still remains the owner of the photo, although he usually gave the company a lot of rights regarding usage.

This is very different from the approach in the USA, where a person can actually sell his ownership of data. In the area of copyright and intellectual property this leads to a lot of issues between the USA and the EU.

As a result of this philosophy a company can only collect and distribute data in a way that was approved by the owner. If he doesn’t agree then the company is not allowed to collect the data in the first place or give the data to a third party. The data owner also needs to be made aware of the involved third parties. It is not sufficient to describe them for example as “other entities within our corporation”, but instead they need to be listed with their full legal names.

The most important issue here is that all of the time the company is responsible for the security of the data, even if it allows a subcontractor to process it. If the subcontractor breaks the law then the data owner can hold the company legally responsible. It is therefore not possible to circumvent the data protection legislation by utilizing subcontractors outside the EU.

The next point that needs to be considered is that data can only be collected for a certain, well defined purpose. It is not legitimate to create to create databases for undefined future purposes. The data owner also has the right to cancel his permission at any time; the data can then not be processed anymore except to fulfill an existing contract.

Since personal data will probably be used to make business decisions about a person, the regulations give the data owner the necessary rights to make sure it is correct. Every person has the right to ask the company about the data that is stored about them and this information has to be given in an understandable way, for example need abbreviations to be explained. This covers all available personal data, including audio, video and emails.

The person also has the right to have wrong entries corrected and to have the data deleted if it is not needed anymore to fulfill legal obligations. The desire for a company to keep the data for later analysis is not a valid reason to keep data infinitely! This right to inquiry and correct personal data can not be waived.

The data also needs to be protected according to its value and state of the art of the storage means. This protection also includes the responsibility to protect against accidental destruction of data. A working and tested backup strategy is therefore imperative.

2.2.2.1 Register

To manage and control the data processing in each country, a national register has to be established [3, art. 28].

Any entity that wants to process personal data has to register its applications and their purpose [3, art. 18-19] before they can be used. To simplify the process the national authorities can publish predefined templates with common applications.

Certain very sensitive applications, as defined by each member state, need an up front audit and approval before they may be used [3, art. 20].

2.2.2.2 Requirements to process data

The EU legislation demands therefore three pillars for a legal application:

1. there has to be a legitimate cause for the processing
2. the data owner approved it
3. the application has been registered (or is based on a legitimate exception)

Only if all three points apply can the personal data be collected and processed.

2.3 Logging and surveillance

Although the EU legislation does not specifically mention log data, it has to be considered under “personal information”, as soon as a person can be identified by it. This means that it has the same protection as any other person related data.

Apart from the EU requirements have some countries enacted specialized regulations in regard to video surveillance, even distinguishing further between digital and analog media.

2.4 Copyright

The issue of unlicensed copies of various kinds in combination with modern information technology has led to difficult legal situations. The EU has tried to recognize this by differentiating between the acting party and the provider of a (transport) service.

Since this is a vast legal field only that part which affects data protection and IT operations shall be investigated. A detailed report with further information has been compiled by the EU in 2006 [28].

2.4.1 Rights of the creator

The directive [11] covers the rights of the creator over his work, and how he can protect himself against misuse. The creator can not sell this right, but rather only gives out licenses of various degrees to allow the usage of his work.

A business is affected by this directive as soon as an employee or subcontractor creates a piece of work for the commercial usage of the company or if third party property needs to be used, such as product pictures or manuals.

2.4.2 Databases

The EU recognizes that, although databases often consist of public information, the creation and maintenance of this collection is an effort in itself [4, art 0.7]. It therefore protects the structure, but not the content or used tools, as an intellectual creation. Still the threat of an user simply extracting all the data and recreating a slightly different database has also been noticed, and therefore any transfer with such an intent is forbidden [4, art. 7.5].

2.4.3 Computer programs

Any form of a program, be it binary or source code, has been recognized as a work of art and therefore has the same protection as a literary work. Unlike in other legal systems only the expressed program is protected, but not the ideas or algorithms behind it [2, art 1.2].

Unless otherwise contractually stated, are for any kind of program created by an employee all exploitation rights automatically assigned to the employer. This does not cover subcontractors, therefore a distinct contractual clause is required here. In any case should a specific contract also be made with regular employees, since even programmers might create work other than code, e.g. draw an icon or a logo, which would otherwise be protected under the copyright.

Furthermore it is legal within the EU to reverse engineer a program for interoperability purposes, if the required information is not available in another way.

2.4.4 Third party transport

According to [8, § 12,13] has the provider, who only transfers or caches on a technical level information, no responsibility for the transported data. [8, § 14] also exempts hosting providers from liability, as long as they remove incriminating data as soon as they become aware of it.

A similar exception is done in [11, art. 5.1.a] which exempts a transport provider from liability for copyright violations.

2.5 E-commerce and signatures

Two areas are distinguished here by the EU:

- plain virtual commerce, such as providing services or goods over the Internet
- classical commerce, but utilizing virtual services as a tool

This differentiation has in parts historic reasons, since selling over a distance was possible by phone already for a long time. Today those two areas are covered by the “Directive on electronic commerce” [8] and the “Directive on the protection of customers in respect of distance contracts” [5]. In practice any company who wants to conduct business by using the Internet will be affected by both.

2.5.1 Electronic commerce directive

The EU wants to establish the “country of origin” principle, which states that a company only has to follow the legal regulations of the country it operates from to be allowed to conduct business within the whole EU. This is especially important for business over the Internet, as customers from various countries should be able to trade with a supplier, without requiring him to have specific knowledge about the legal situation in each of their countries. A detailed analysis can be found in [159].

According to [8, § 0 lit. 58] only service providers within the EU are affected. To determine the location of the service provider it is relevant from where his business operates, not where his physical server infrastructure is located [8, art. 2c].

It should be noted that already advertising or general information is covered by this directive. It therefore not only applies to classic web shops but rather to any web site offered by a commercial party.

2.5.1.1 Information requirements

A service provider has to provide the following information in an easy and understandable way to his customers [8, art. 5.1]:

- person or company name
- geographic address
- contact information for quick communication, including the email address
- if applicable commercial register number and relevant court
- if applicable the regulating authority
- if applicable informations about professional regulations
- if applicable the sales tax number

For any pricing information it has to be made clear if taxes are included and if shipping costs are included [8, art. 5.2].

In regard to commercial communication, such as email, is the sender required to make it clearly visible that the purpose is commercial and also who the sender is [8, art. 6].

To prohibit unsolicited commercial communications (often called “spam”) originating from the country with the least legal protections, [8, art. 7] requires all member states to ensure that the sender of the communication is clearly visible and respects existing opt-out registers.

Furthermore [5, art. 10] forbids "cold calls" by automated voice systems as well as fax advertising without prior consent of the other party. Otherwise advertising, for example by email, is allowed as long as the recipient does not state his disagreement, which is therefore an "opt-out" system. Member states may implement more strict rules.

2.5.1.2 Order process

The service provider has to make it clear to the customer [8, art. 10]

- how the process of creating an order works and at which point a contract comes into existence
- if the customer will have access to the contract text afterwards
- the technical means to prevent entry errors made by the customer
- the available languages

The customer also needs to have access to a copy of the general terms and conditions in a persistent form.

Unless the communication is done entirely by email or similar tools, the service provider has to

- provide adequate tools to allow the customer to spot and correct data entry errors made by himself [8, art. 11.2]
- confirm the acceptance of the order [8, art. 11] immediately to the customer. This should prevent from providing misleading information which might trick a customer into entering a contract that he had no desire to. Both, the order and the acceptance notification, are considered delivered if it is possible for the receiving party to retrieve them. In practice this means that, for example, an email is delivered if it arrives at the recipient's mail server, although he might not have retrieved it yet.

2.5.2 Distant contracts directive

Apart from general information requirements, similar to the electronic commerce directive, customer rights are defined here.

The commercially most important one is that the customer has for seven days the right to cancel the contract without providing reasons. The only costs which he has to bear are those for returning (sending) the received goods. In case the provider has failed to provide all required information according to [5, art. 5] upfront, this time period is extended to three months. In any case has the provider to return the customer payments within 30 days without deducting any charges.

Exemptions to this right are defined in [5, art. 6, lit. 3], most notably if the customer has agreed that the provision of the agreed service shall start within those seven days or if the product has been customized to him.

2.5.3 Digital signatures

Signatures are the digital equivalent to signing by hand. The system usually consists of two related keys: a private key, which is only known to its owner, and a corresponding public key that is readable by everyone. The mathematical background behind those keys allows this person to sign documents with the private key, which can then be verified by everyone using the public key, thereby proving the authenticity of the signature and the integrity of the signed document. Digital signature systems are standardized by the IEEE [160] and are widely in use in IT systems.

The EU has, based on this, created a directive [7] to enable Europe-wide digital signatures that can be used to legally sign contracts. This directive describes the framework around the certificate management and how to implement their legal status to put the same value onto them as on handwritten signatures. Therefore any further commercial legislation can be applied as before without any modifications for digital signatures.

2.5.4 Electronic invoices

As part of the value added tax system [26] the EU also mandated how a valid invoice has to be done. While this allows also for electronic invoices by using digital signatures, the practical usage has been severely limited through different implementations in different member states. In some of them the requirements are also very high, thereby constituting a considerable entry barrier for SMBs.

The EU has recognized those issues and therefore made an amendment in 2010 [27, art. 233], which now allows the business parties to agree on the requirements for electronic invoices themselves, instead of mandating them through a government authority. It can be assumed that this will lead to a higher acceptance of electronic invoices, but it has to be noted that this amendment has not yet been implemented into national law in Austria or Sweden as of September 2010.

Chapter 3
The legal situation in Austria

3.1 Overview

Austria implemented the EU directives by using nearly the same structure as in the EU documents. For someone with a sound knowledge of the EU regulations will it not be a problem to understand and apply the Austrian version.

3.2 Implementation of the EU directives

3.2.1 Data privacy act

The directive for protecting personal related data has been implemented in the "Datenschutzgesetz 2000" (DSG [31], data protection act) and the management of the data processing registrations and other duties related to personal data are done by the "Datenschutzkommission" (DSK [45], commission for data protection). The detailed execution of the DSG has been published in three additional acts:

- Act about adequate data protection in third countries [30]
- Act about the data processing register at the DSK [33]
- Act about template applications according to the DSG [40]

It is worth noting that the DSK consists of only 20 people, with some of them working part time. It is therefore considerable underfunded which, according to their own report[47, p. 24ff], hinders them in fully executing their duty. Although the commission is by law independent [31, § 37 art. 1], this has to be questioned as some of the executive members are located in the offices of the federal chancellor and some part time employees are also employed by the Austrian government in other positions.

Austria also has the "Datenschutzrat" (DSR [85], data protection counsel), whose duties are defined in [31, §§ 41-44]. Nearly all members are sent by political parties and its mission statement is to advice the government in data protection issues. Since it is therefore by far not independent but also according to [31, § 35 art. 1] responsible for the supervision of the Austrian implementation it can be argued that this is in violation of [3, § 28 art. 1]. But so far no legal objections have been raised.

There are also some non-governmental organizations which are related to the area of data security and privacy, with the most well known of them being "ARGE Daten" [83]. Since the DSK is not considered independent in the public opinion, ARGE Daten is often used as the focal point for complaints in regard to privacy or data protection. They also offer training courses for applying the regulations in a business environment.

3.2.1.1 Data protection

According to [31, § 1] any processing of personal-related data is prohibited, except for clearly defined purposes:

- with the acceptance of the person or if he has vitally important interest in it
- overriding and eligible interest of a third party
- according to the law
- if the data was already in the public

3.2.1.2 Data protection officer

A data protection officer, like in other countries, is not required or even defined within the DSG. If one is installed by a company then he has no legally binding rights or duties. In some cases a contract ("Betriebsvereinbarung") with the local workers' union can be used instead to avoid asking each individual employee.

3.2.1.3 Groups of data

Apart from the types of data as defined in the EU directive

- sensitive data [31, § 4 lit. 2] ("sensible Daten"), which covers data of a very private nature; for this no third party can claim any eligible interest
- personal related data [31, § 4 lit. 1] ("personenbezogene Daten"), this is the same as in the EU directive

Austria also introduced additional types

- specially protectable data [31, § 18 art. 2] ("sonstige besonders schutzwürdige Daten")
- indirect personal related data [31, § 4 lit. 1] ("indirekt personenbezogene Daten")

The general term of personal data has been split up into two groups. "Personal data" is any data, which the data processor can directly assign to a certain person. "Indirect personal related data" on the other hand is any data which actually relates to a person, but the processor could only make this relation through illegal means, e.g. through unlawfully using a third party which might have the information required for a correlation. The aim here is to prevent the transformation of personal data into unprotected impersonal data by introducing a layer or third party, without whom the data can not be directly assigned to a specific person.

The type "specially protectable data" was implicitly introduced in [31, § 18 art. 2] because the original definition of sensitive data didn't include information about convictions, credit scores and other data which is not as private as religious affiliation or sexual orientation, but should still be more protected than other personal related data. This group is not actually defined by a name in the DSG, but has to be considered separately from the others for practical reasons.

One main difference from the directive also exists in the coverage of protection. Whereas the EU only mentions real, physical people, Austria also protects the data of legal entities, for example companies. One implication of this is that it does not make any difference for a business if their customers are people or other companies, the data about them needs the same level of protection.

3.2.1.4 Registration

If specially protectable or sensitive data is affected and the application is not covered by a template application, then the approval of the DSK is required before the application can be used. Otherwise the application can be used as soon as the registration is sent to the DSK.

3.2.1.5 Internal data usage

The DSG of course also applies to the internal usage of personal data within a company. Duties resulting from legal or contractual obligations, such as the payment system, are already allowed by the DSG and don't require further approval.

If there is a workers union ("Betriebsrat") then the company has to make an agreement ("Betriebsvereinbarung") with them in case the company wants to process any further personal information such as systems to monitor and control their employees or others which affect human dignity [29, § 96]. Without a workers union individual agreements with each employee need to be done.

The term “human dignity” has to be considered in a very broad sense. In one court decision [72] it was ruled that a telephone system, which records caller, duration and other properties of a call, makes the employee feel observed and thereby affects their human dignity. An agreement with the workers union was therefore required.

3.2.1.6 Information requests

Everybody has the right to ask a data processor for the information they has about him. The requestor has to provide information about his identity which allows the processor to identify him in his database. The processor has to provide the results within eight weeks after he received the complete request [31, § 26 lit. 4] and he has to provide it on request for free once every year; otherwise EUR 18,89 can be charged [31, § 26 lit. 6].

The requested information has to be kept for four months, even if the removal was requested.

Failure to provide the information in time can be punished by up to EUR 500 [31, § 52 lit. 2a].

3.2.1.7 Penalties

Two categories can be applied:

Delict this covers mostly hacking, misuse of data, failure to delete or correct data and denial of information requests, which can be fined up to EUR 25.000 [31, § 52 lit. 1]

Omission of registering the application or data transfers, or failure to publish information about the purpose of the application, which can be fined up to EUR 10.000 [31, § 52 lit. 2]

Both have a statute-barred prosecution of six months.

3.2.1.8 Changes in 2010

During 2009 changes to the DSG have been discussed and enacted on 30. December 2009 [32], the most relevant points being:

- a party keeps the role of controller even if the subcontractor makes the decision if and how he will use the provided data.
- more precise definition of what a processor or subcontractor is
- to be considered “data collection” does not require anymore the intention to actually use them in an application

- a “data transfer” is now considered in both ways between a controller and processor
- any claims to the DSK of a controller about his processor become legally binding when he registers his data application with the DSK
- it is not necessary to register a manual file under certain conditions
- the registration of a data application has to be done electronically, e.g. by using the “Bürgerkarte” (citizen card [84], a PKI system)
- the registration for non-sensitive handling will be automated by the DSK
- the DSK has the right to investigate into parties who are suspected to be required to file a registration but have not done this so far
- if the controller becomes aware of a systematic and severe misuse of his data, then he is required to inform the affected persons about it
- the legal situation around video surveillance has been better clarified (see also 3.2.2.3)

3.2.2 Logging and surveillance

3.2.2.1 Generic logging

If the logged data is not related to a person then the DSG does not apply. In any other case, even if the relation is only indirect, the data has to be considered person related and therefore the DSG fully applies. It also has to be observed that only as little data as necessary shall be logged (“Datensparsamkeit”, data austerity), since data collection without a purpose is not allowed. Collecting data before it is actually required (stockpiling) is not allowed for private parties, but only done by the government (see also the EU data retention policy [25]).

3.2.2.2 Logging of access

Access to personal data has to be logged according to [31, § 14] to control its validity. Those logs, and others which are acquired on a legal base, are themselves personal data since they relate to a person and need to be protected accordingly. Logs based on [31, § 14] need to be kept for three years and have to be destroyed afterwards.

In any case may logs only be used for their intended purpose, it is forbidden to evaluate user behavior from them or use them in any other way (see also 3.3.2.14). Furthermore may logs only be created in the least necessary amount.

3.2.2.3 Video surveillance

In 2010 the DSG has received additions to [31, § 50] to regulate data collection through video recordings, which are now treated more similar to regular data.

In general is surveillance only allow to protect an object or person, to fulfill legal requirements or if the recorded people gave their consent. [31, § 50a lit. 5] especially forbids video surveillance of employees and their behavior. Furthermore states [31, § 50a lit. 7] that it is not allowed to do an automated search through the videos using pictures (e.g. "known suspects") or by criteria which consist of sensitive data (e.g. skin color).

Any recorded video, if not covered by a legal requirement, has to be deleted after 72 hours [31, § 50b lit. 2] (weekends and public holidays are excluded).

The video system has to be registered with the DSK, unless it does not record or only records on analog media [31, § 50c lit. 2].

The controller has to make the fact of the surveillance visible in a way that potentially affected persons can avoid this physical area and he also has to make it clearly understandable which legal entity is the controller.

A data inquiry by an affected person has to be answered with a copy of his video. If this is not possible because rights of a third party might be affected, then he has to receive a masked video or a written description of it.

3.2.3 Copyright

The term "copyright" is not in use as such, instead the legal base is the "Urheberrecht" (right of the originator).

All three of the relevant EU directives ([4], [11], [2]) have been integrated into the "Urheberrechtsgesetz" (UrhG[43]) without any relevant alterations.

3.2.4 Imprint

Any website published in Austria also has to conform to the "Mediengesetz" (MedienG [36], media act) according to [36, § 1 lit. 5a].

This requires [36, § 24] the publisher to provide his name, city of residence and purpose of the site in an easy accessible way.

Companies are furthermore affected by the "Unternehmensgesetzbuch" (UGB [42], business act), requiring them [42, § 14] to publish the following information:

- company name
- company register number and responsible court
- geographic address
- legal form

This has to be done on all public communication, including all websites and also all external email communication.

To simplify the situation, the Austrian Chamber of Commerce provides a web page per company with all the required information, which can then be linked to [88]. It still has to be taken care that the information is up to date and complete.

3.2.5 E-commerce and signatures

The e-commerce directive [8] has been implemented in the Austrian “E-Commerce Gesetz” (ECG [34], e-commerce law). One relevant alteration has been made, as the wording of the directive aims at interactions between businesses, whereas the ECG covers electronic business in general [34, § 1 art. 1], thereby covering transactions between private and business parties alike.

3.2.5.1 Information requirements

[34, § 5] implements the [8, art. 10] requirement for the service provider to publish his relevant business and contact informations as well as a downloadable copy of his general terms and conditions (“AGBs”). It should be noted that common abbreviations, such as “FB” (“Firmenbuch”) or “HG” (“Handelsgesetz”) may not be used here as they don’t fulfill the requirements.

If the client is a consumer then he furthermore has several rights under the “Konsumentenschutzgesetz” (KSchG [35], consumer protection act), the most notable being the right of withdrawal within seven work days, about which he has to be informed prior to confirming the contract. Failure to provide those informations extends the right of withdrawal to three months. The consumer has to pay for the transport in such a case, if this was agreed upon in the contract.

3.2.5.2 Spam protection

Private and also commercial entities can sign up on the “Robinson Liste” [90], which is operated by the “Rundfunk & Telekom Regulierungs GmbH” [91], a government-owned company. According to [34, § 7 art. 2] this prevents other parties from sending them commercial communication (“spam”). Since this list therefore needs to be accessible by any commercial party within the EU, it might be misused to illegally obtain email addresses, as the RTR themselves notes.

Still any commercial party needs to query this list during marketing campaigns as they might be otherwise subject to legal actions by the recipient.

Unlike the EU directive, which describes an "opt-out" system, Austria has implemented an "opt-in" system for emails and other communication forms [41, § 107]. The only exceptions to this are if

- the sender has acquired the contact information during a prior commercial transaction and
- it is used to advertise a similar product or service and
- the recipient has an easy and cost free way to stop this (going into "opt-out") and
- the recipient is not already on the "Robinson Liste".

3.2.5.3 Hyperlinks

The ECG covers the linking to informations held by other parties in [34, § 17], which has no equivalent in the directive.

A party who links to external content can not be held responsible for this content if

- they don't claim it as their own and
- the external entity is not under the party's control and
- the link is removed immediately if the party becomes aware of the illegality of the content.

3.2.5.4 Signatures

Austria implemented the directive [7] in the "Signaturgesetz" (SigG [38], signature act) and its daily operation in the "Signaturverordnung" (SigV [39], signature order). Responsible for the Austrian signatures is a department of the RTR [92].

The SigG itself is technology neutral, but refers to signatures and private/public cryptographic information. The SigV on the other hand defines the approved mechanisms in detail, such as, for example, that RSA, DSA and elliptic curve may be used in an asymmetric key setup.

Certificates of other suppliers from within the EU are considered legally equal to the Austrian ones [38, § 24 art. 1].

3.2.5.5 Electronic invoices

The main use of signatures is for, usually high volume, invoice exchange, as this allows for cost savings in regard to printing, handling and archiving.

Since 2003 such invoices are accepted by the Ministry of Finance [44] if they

- are signed according to [38, § 2 lit. 3] or

- are transmitted electronically, as agreed by both parties, and a summary is also exchanged on paper or signed according to [38, § 2 lit. 3].

The invoices need to be immutable, show the verifiable originator and have to be kept for seven years, similar to paper invoices. A printout is not sufficient since the digital signature can not be verified from it. Also both parties need to agree to the electronic exchange, otherwise paper invoices have to be used.

If a party does not have it's own ERP and PKI infrastructure then they can use the "Bürgerkarte" (citizen card [84]), which is part of the Austrian public PKI, to verify or sign single documents.

Further hands-on information is provided by the Austrian Chamber of Commerce at [86] and [87].

3.2.6 Electronic communication networks

The four EU directives ([14, 15, 16, 17]) have been implemented in the "Telekommunikationsgesetz 2003" (TKG 2003 [41], telecommunications act). It regulates how communication networks may be provided, their accounting responsibility and data protection duties.

Although this mostly aims at service providers, such as telecoms or Internet providers, any other company might be covered by it as well if they provide public communication networks such as free wireless Internet access. This also leads to further responsibilities such as providing informations to the police [37, § 53]. It has to be noted that there is no legal certainty for this whole complex until now since a lot of questions have not yet gone up to the highest court [89] and also since Austria has not yet implemented the EU directive about data retention [25].

3.3 Local court decisions

3.3.1 OGH legal rules

The following overview includes all existing OGH legal rules up to April 2010 in regard to the DSG, except for [79], [70] and [69] which are not of particular relevance here.

3.3.1.1 Data deletion and correction [82]

The respondent collects public information about credit ratings in a database and provides access to this information to a single company, who in turn offers this together with other sources to the public. The plaintiff was denied a mobile phone contract because of this information, whereupon he requested from the respondent to delete one record about him from the database, which was refused by the respondent.

The OGH decided that the respondent has to delete, on request, parts of the collected data even if this would be inconvenient, since the respondent always has the freedom to delete all data about the plaintiff anyways.

The respondent also tried to claim that he is merely a processor according to DSG and the other company is the controller. This was denied; since both of them collect and provide the data they both have to be seen as processors.

Furthermore the respondent argued that he provides the data only to one customer and even then only against payment, therefore his database can not be considered public. This view was not seen as correct. Since everybody could buy access to this data for EUR 25 through the other company, his database must be seen as public and the DSG fully applies.

3.3.1.2 Public databases [80]

The OGH defined in some detail in which case databases have to be considered public according to the DSG. Only if the access is restricted to a well defined, closed community it may be non-public. As soon as in theory everybody can gain access to the database, for example by paying a fee or becoming member in a group, the database has to be considered public.

In one case a company operated a credit score database to which only their clients, typically banks and mobile phone companies, had access via a VPN line and personal login. Still the OGH considered this to be public, since the company, based on their own decision, could at any time allow new members to this group. The company was also considered as a controller and not just a processor since it collected the data and provided it to its customers.

3.3.1.3 No justification required by client [81]

The controller of a database argued that, although the affected person may request the deletion of records without any justification, he still has to provide one on request. This view was denied, as records have to be deleted on request without any further justification.

3.3.1.4 Usage of public contact information [78]

The plaintiff is the leader of a public commerce alliance and as part of his work has published on their web page and print publications his email address and private mobile number, often with the invitation to contact him. The respondents used this information during a political campaign to invite citizens to write him and tell their opinion. The plaintiff was then overwhelmed by the amount of emails and requested that the respondents “stop this”.

It was decided that since he published the contact information, and even kept doing so during the law suit, this information has to be considered public and the case was therefore dismissed.

3.3.1.5 Representative [77]

In this case the workers union of an airline company tried to sue their employer for using personal data in their employee management system without getting permission from every employee first.

The OGH denied this case for two reasons. First, the workers union as a representative can’t sue based on the DSG since this can only be done by the affected individual personally. Second, the workers union has already certain rights within the company as a representative and by having influence on the business processes the permission of the individuals is not necessary.

3.3.1.6 Upfront information [76]

If a person has a record in a credit score database, this might cause negative effects for him in the future. The controller or provider of such records is therefore required to inform the person that his actions, e.g. having overdue bills, will result in such an entry. This allows the affected person to challenge and correct any false informations about the situation.

It can not be claimed that the companies who use the credit score database have a justified interest in processing this data and therefore don’t need to inform up front.

3.3.1.7 Specific information [71, 74]

The information of the affected person can not be done by rather unspecified clauses, such as “entry into a warning list”, but it has to specify the complete name and controller of the database. It has to be clear who will receive the information and under which circumstances.

This privilege to transfer information also has to be clearly and obviously stated, it may not be hidden within the general terms and conditions. The average reader must be aware which information might be transferred to which party.

3.3.1.8 IP addresses [75]

This legal ruling defines that IP addresses, no matter if static or dynamic, have to be considered customer master data for an ISP and they are therefore not protected as information in transfer. They can therefore be obtained and correlated to a name in the same way as the full name or address of a customer, which usually is done through a law suit.

3.3.1.9 Private information [73]

A person provided private information about himself to a closed audience in a pub, which was then used by a police officer for other purposes by claiming that it was now public information.

The OGH denied this view, since the audience was only a very small group and the affected person did not have the intention to provide it to the general public.

3.3.1.10 Legal and physical persons [66]

Although the Austrian implementation also covers legal persons, thereby companies, they can not always apply the DSG to keep their personal information secret. Especially business law requires them to publish their financial statement and other information.

3.3.1.11 Definition of “database” [68, 67]

Here the definition of a database (“strukturierte Sammlung”, structured collection) is made, since the DSG only applies to those.

The OGH defines it as any collection that is organized or can be searched by at least one criterion, no matter on which media it is stored. Therefore even paper collections are covered, if they are for example organized by alphabet. The only exclusion are unsorted collections, such as paper files without order or a single expert’s opinion.

3.3.2 DSK decisions

3.3.2.1 Video cameras in council housing [48]

The city of Vienna provides flats in some large housing areas. There has been some considerable vandalism in the public areas, for example at the trash bins, and it was considered to install video cameras as a prevention against this.

After several discussions the DSK ruled that

- it is not allowed to monitor the entrances and the staircases, since this would be a severe intrusion of the tenants privacy and also has no relation to the vandalism that shall be prevented
- it is allowed to monitor the area of the garages and trash bins where vandalism occurred
- the video recordings can only be examined if vandalism has happened, a permanent viewing is not allowed, and the recordings have to be deleted after 72 hours if not needed in such a case
- a statistic has to be created about the acts of vandalism that were recorded and brought to court
- the installation is limited until 31.12.2009

After this deadline the DSK will compare the statistic from the surveillanced houses against those of houses without surveillance and then consider if the cameras can stay in place.

This is a good example to show the intention of the law, as the city of Vienna has to show that is has a rightful need to collect the personal data, in this case video recordings of the tenants, because otherwise it couldn't protect its property. Especially the ruling that only affected areas are allowed to be monitored make it clear that there can not be a general data collection without specific purpose.

3.3.2.2 Video surveillance at a company [52]

A ministry applied to the DSK to be allowed to install video surveillance cameras in its building. Although parts of the decision apply only to the public sector some details are also relevant to a company environment. The surveillance was allowed, with some restrictions:

- The video cameras may not record any public space, such as the pavement in front of the building, unless it can not be avoided, and even then it has to be kept to a minimum.
- Any recording has to be encrypted and may only be kept for up to two weeks.
- The records may only be evaluated if one of the cases described in the application takes place. This means that a routine inspection of the video files is not allowed.

3.3.2.3 Manual file [49]

The plaintiff appealed to the DSK to gain access to his personnel file which his employer, the Austrian government, kept. He assumed that a certain psychological report in there has caused a negative effect on his career.

The file itself is a unsorted collection of various papers about the employee, only the files themselves are sorted by the employees names.

The DSK therefore ruled against the plaintiff stating that the Austrian definition of file is taken from the EU directive which states

> whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive [3, § 0 art. 27]

Although the files are sorted, their content is not. It has no specific structure, but is rather a collection of loose papers. Therefore it is not covered by the data protection act and the employer does not have to provide him with information about the content.

This ruling was confirmed by the Austrian Supreme Court.

It has to be noted that he still has the right to see the content of this specific file according to the labor legislation, but not as he requested according to the data protection laws.

3.3.2.4 Usage for other purposes [50]

After staying at a hospital for medical treatment the plaintiff received, as part of a larger group, a letter from the hospital asking for a donation. Since he assumed (correctly) that the hospital took his contact information from his last stay, he appealed to the DSK that his personal data was misused because it should only be processed during his medical treatment.

The DSK ruled against the plaintiff, because the data was collected in a legitimate way (medical treatment) and later on used by the same party for a kind of advertisement of its own medical services. Although this is not the exact same use as the original cause, it can still be considered compatible.

It was further noted that it would not be legitimate to add the information if he has donated money to his patient file.

3.3.2.5 Information request [51]

An employee of the Austrian government requested from his employer a list of all information that has been recorded about him.

Part of this was the request for Internet log files. The employer keeps a sequential log of any Internet access from within the network and also a log of logins to the PCs. Therefore this log information has to be considered personal data, since it can be related to a specific person.

The employer argued that the access log is only kept to support legal actions in case of misuse and that it can only be searched sequentially. Therefore the information request can not be fulfilled since it would cause considerable costs.

The DSK rejected this argument, because as stated the employer would search the log in case of legal actions and therefore he is willing to accept those costs. For the same reason he has also to accept the costs in case of an information request.

3.3.2.6 Information request and correction [53]

The plaintiff requested that the controller of a database, in this case a marketing company, lists all his records and deletes them. The company just "locked" his records and asked the plaintiff for more clarification about why and upon which incident he wants to have the records deleted.

The DSK decided against the company, since the plaintiff only has to request the deletion by specifying how the controller got hold of his data. The controller can not put more work onto the plaintiff, even if it might cause more effort for themselves. Furthermore the plaintiff does not have to prove that any further data transfer has been done, rather the respondent has to provide a list if there have been any such.

3.3.2.7 Language of information request [54]

The DSK stated that any request to them has to be done in German since this is the official language for Austria. In this case a request was done in Italian and English, and it was therefore denied.

3.3.2.8 Timeliness of information request response [55]

The controller has according to the DSG eight weeks of time to respond to an information request. In this case the response did not include all data, therefore the DSK ruled that after eight weeks the controller has not fulfilled his obligations.

3.3.2.9 Data processing outsourced [56]

The respondent answered to an information request by the plaintiff that he can not provide any data since this is in whole done by another company, in this case a tax consultant. He himself does not process any person related data. The DSK denied this argument since the respondent gave the other company the order to process the data and therefore he is still the controller of it. The respondent as the controller has therefore to answer the request, even if he has to acquire it from his subcontractor first.

3.3.2.10 Unstructured data and time of request [57]

In this case a company hired a private investigator to find an information leak, who afterwards provided a paper report about the suspected person. This person found out about the observation three years later and filed an information request against the company and the private investigator to find out what kind of information about him has been collected, which was not fulfilled in both cases.

His complaint was denied by the DSK because at the time of his request any data about him did not exist anymore on the private investigators IT system. Furthermore the report only existed in unstructured paper form and therefore was not covered by the DSG.

3.3.2.11 IT Subcontractor outside the EU

Two companies applied to be allowed to process person related data at a subcontractor in the USA [58, 59]. Both requests were approved by the DSK since they could show a contract which included the EU standard contractual clauses [13] and therefore assured a sufficient protection for the data.

Similar decisions have been made in regard to outsourcing to Turkey [60] and India [61].

3.3.2.12 Form and wording of a data inquiry [62]

The plaintiff asked a bank about a specific query of the credit register which seemed to have taken place without him having any relationship with the bank. Since the answer of the bank did not satisfy him, he filed a complaint to the DSK regarding an incomplete request for information according to the DSG.

The DSK denied his request, since from the text of his request it was not obvious to the bank that he wanted to receive information according to the DSG.

3.3.2.13 Credit rating inquiry through subcontractor [63]

In this case a business used a rating company to decide if a new customer was credit worthy. The rating company holds records of the credit history of a person and calculates a yes/no answer according to a logic predefined by its customers. The plaintiff filed an information request against the first company, which they answered by stating that they only keep his static records, such as name and address, and a yes/no credit score. Everything else is at the rating company and they can therefore not give any further answer. Even the algorithm behind the yes/no answer can not be stated since this is done at the rating company.

The DSK denied his complaint, since the given response was correct and complete. But they also stated that he has the possibility to file another request against the rating company to receive the information he probably was interested in.

Furthermore it was stated that if he would also request informations about how the yes/no credit score was (automatically) generated, the first company will have to explain this in detail. This arises from the fact that this company defines the algorithm herself before providing it to the rating company, which makes them the data controller in this case and the rating company the processor. They therefore have full responsibility according to the DSG since the data is (logically) transferred to them.

3.3.2.14 Evaluation of IT systems activity logfiles [64]

The plaintiff was an employee of the Austrian tax office and was about to apply for a higher position. As part of his evaluation for this position the anti-corruption officer made a logfile analysis of the plaintiffs data access of the past eight years to evaluate his behavior patterns. Since some private queries were found the plaintiff had to face negative consequences. As a result of this he filed, among other points, a complaint about misuse of data , in this case logfiles.

The DSK approved this point of his complaint. Any data controller has to keep access logs for three years, but not longer. Also this information may only be used to monitor misuse of the system, but it can not be used to gather information about the behavior of a person

3.3.2.15 Webhoster is processor [65]

In this case the respondent used a web hosting company to provide access to person related data against payment, but failed to state this fact and therefore also the identity of this web hoster to the plaintiff.

The DSK stated that according to the DSG even the saving of data makes an entity into a processor, therefore the respondent has in this case the role of the data controller and the web hoster has to be considered a processor and subcontractor.

Chapter 4
The legal situation in Sweden

4.1 Overview

Sweden has long been known to be one of the leading social states worldwide. The government provides many services for the citizens which therefore requires it to collect and process a lot of personal data. The core concept of the data protection legislation is therefore to protect individuals, which also shows in the term “personuppgift” that translates to “information about a person”.

Another Swedish institution is the “ombudsman”, a contact person who is supposed to settle disputes, usually between a customer and a service provider. In regards to data protection the “Datainspektionen” [144] has been given this role, among other duties. It is therefore also politically recognized as a valuable institution and receives sufficient funding for its work. Currently they employ more than 40 people and also provide a telephone hotline for concerned citizens.

The Swedish government works according to the publicity principle (“offentlighetsprincipen”, [93, ch. 2]). This makes any document within the government, with some exceptions, accessible to the citizens and is codified in the “Offentlighets- och sekretesslag (2009:400)” ([110], publicity and secrecy act). Of course this sometimes leads to the disclosure of personal data since it may be part of official databases or documents, but this usage is covered by the Swedish implementation and therefore legal.

Also journalism is of high public value which results in a very good protection of newspapers and other means of publishing. As a side effect of this a lot of the privacy protections might actually not apply if certain conditions are met (see 4.2.2.4).

4.2 Implementation of the EU directives

4.2.1 Overview

The Swedish implementation is split up into three parts, covering the data protection, the processing of it and the supervising body.

4.2.2 Personuppgiftslag (PuL [100], Personal Data Act 1998:204)

This is the Swedish adaption of the EU Directive 95/46/EC [3] and therefore has a similar structure. It is in general often less specific than the EU directive and leaves the implementation details mostly to Datainspektionen.

One important fact is stated in [100, § 2], which says that other, conflicting, laws have precedence (lex superior) before PuL. The most important example is the law for official statistics [104], which allows the publishing of every citizens income report. Whereas this would be secret information in most countries, every Swede can download the tax report of his neighbor. Other examples are government statistics about the income per occupational group or geographical area.

In [100, § 3] the law is limited to information about living natural persons which further shows the intention to protect the citizens. After ones death the personal data is therefore not covered anymore by the PuL! Furthermore no distinction is made if the information can be directly or indirectly linked to a person, both cases are considered personal data.

[100, § 7] excludes personal data from protection if it is used by the press. Sweden has in general a very good protection of the freedom of the press and freedom of speech, and here again this overrules the PuL. It has to be noticed that this is limited if the information is published on the Internet, as this would allow access from outside the EU; an example will be shown in 4.3.1.

Sweden has introduced [100, § 11] that is not found in the EU directive, which explicitly states that the use of private data for direct marketing purposes is not allowed if the affected person forbids the processor in written to do so.

Under certain circumstances, most importantly by approval of an official ethics committee, does [100, § 19] allow the processing of even sensitive personal data without the consent of the persons for statistical or scientific purposes.

[100, § 20] prohibits the processing of information about legal offenses, unless stated otherwise. So far the most well known exception has been to allow Antipiratbyrån [141], a private organization working against software piracy, and the IFPI [151], a private organization that works against audio copyright violations, to collect personal information about people who are suspected to be exchanging unlicensed material by means of file sharing [145].

Every Swedish person has a "personnummer" (personal number), which is a unique identifier. This is widely used to identify e.g. customers, and although it is personal data it is not really considered secret. [100, § 22] therefore allows for processing of this ID without the consent of the affected person if it is needed to securely identify the person or for other important reasons.

Any inquiries to a processor need to be answered with one month, or, if there are special reasons, within four months as specified in [100, § 26]. It is required to request this in written and signed by the affected person.

[100, § 28] defines that if a decision in regard to a person is automatically made based on personal data, then the processor can be required to describe based on which data and according to which logic this decision was made. This is not an exact implementation of the EU directive and gives the affected person more rights than intended on the EU level.

In [100, § 31] the necessary security measures for the processor are defined. This is worded rather general and leaves out the detailed list of the EU directive, especially the need to protect data against accidental loss is not mentioned here. On the other hand gives [100, § 32] Datainspektionen the power to define the necessary measurements for the processor and fine him [100, § 45] if he doesn't comply. This can be seen as a very practical implementation of the EU directive as it allows the group with the most hands on experience, Datainspektionen, to create fitting rules for each real life situation.

Sweden uses the possibility to define a personal data representative (PDR, "personuppgiftsombud") in [100, §§ 37-40], who is an employee of the processor but needs to be independent enough to supervise the data processing. He takes partly the role of Datainspektionen and therefore it is not necessary anymore to notify them of new data applications. Instead the PDR has to keep track of the internal data usage and make sure that any processing is according to the law; when in doubt he has to contact Datainspektionen. This exemption does not apply if the personal data is about sensitive data, such as genetics, taxes or law enforcement. He should also be the contact person for third parties in case data needs to be corrected or removed [100, § 40]. In case of a misuse it will still be the processor who has to compensate the person, not the PDR [100, § 48].

4.2.2.1 Datainspektionens föreskriftet 2001:1

How PuL is applied in practice is defined by the rules Datainspektionen publishes. In [149] the exceptions from the compulsory registration of data applications are defined, such as:

- If the data is processed with the consent of the person.

- If the controller himself keeps a register and the data
  - is not sensitive and about membership, employees or customers, or
  - is about sick leaves of employees for payroll purposes, or
  - is required by the employer to fulfill legal obligations.

4.2.2.2 Förordning (2007:975) med instruktion for Datainspektionen (DIFS [108], ordinance for the data inspector)

This lays ground for Datainspektionen, the Swedish implementation of the supervising authority requested by the EU directive [3, art. 28], although the details of its responsibilities are codified somewhere else [101].

In [108, § 1] it is explicitly stated that this institution is not barely for the management of the data processing register, but that it also should monitor and advice on upcoming technical developments as well as provide support for PDRs. It is furthermore responsible for cooperating with the EU Schengen, TIS and Europol groups [108, § 4].

4.2.2.3 Personuppgiftsförordning (PUF [101], personal data ordinance 1998:1191)

Here Datainspektionen is defined as the responsible institution for the supervision of the processing of personal data [101, §§ 1-2] as well as the details of it's duties and rights.

[101, §§ 3-5] state again the exemptions under which data processing does not have to be registered, especially noting the Freedom of the Press Act.

Although sensitive personal data can be used for statistical or scientific research [100, § 19], [101, § 10] requires the processor to apply at least three weeks in advance to Datainspektionen even if an ethical committee has approved the processing.

Organizations representing a certain branch or sector can utilize [101, § 15] to request an opinion from Datainspektionen during the development of a branch agreement on data processing.

[101, § 17] introduces the right for each Swedish citizen to ask Datainspektionen for support in regard to the EU directive (stopping the processing of personal data [3, art. 14]), if the processor is located outside Sweden but covered by the directive.

4.2.2.4 Utgivningsbevis

Sweden places a high value on the freedom of speech, giving it even priority over PuL. This effect is caused by the "utgivningsbevis" (publishers certificate), which states that the owner, which can be a person or legal entity, acts as a publishing source. Its legal base is [93] and [95], and it can be obtained from "Radio- och TV-Verket" (radio and television authority [153]) for SEK 2.000. The owner of the certificate will then be put under special legal protection as a journalist, basically disabling any PuL liability for him in regard to published content.

The requirements for this certificate, in case of a website, are [95, ch. 1 § 9]:

- the publisher is identifiable and a resident of Sweden, and
- the origin of the distribution is in Sweden, for example the server location, and
- it is accessible by the public, and
- the content comes from a database which only can be modified by the owner of the certificate, whereas a website is considered such a database, and
- the name of the distribution (such as the website) is unique in a way that it can not easily be confused with another entity.

Although the publisher needs to be named on the website, any person creating content and publishing it there has the right to anonymity [95, ch. 2 § 1]. The publisher has no legal obligation to disclose their identity. This goes as far as even having a state entity, such as the police, asking for the identity is illegal [95, ch. 2 § 2].

4.2.3 Logging and surveillance

In general the Swedish laws try to define the requirements for video surveillance in a rather generic sense, and it is then the duty of the authorizing entity to decide in each specific case about the details of the surveillance system.

4.2.3.1 Lag (1995:1506) om hemlig kameraövervakning [96]

This law regulates the usage of hidden video surveillance for the prevention of crimes which are punishable with at least two years of prison. The surveillance may only be done as long as necessary, but topmost one month [96, § 4].

Any surveillance needs to be applied for at the local "länsstyrelse" (county administrative board) which might approve it only with detailed restrictions.

4.2.3.2 Lag (1998:150) om allmän kameraövervakning [99]

If the surveillance camera is to be public visible then it will be covered by this law.

In general need the affected persons to be made aware of a camera by a sign before they enter the camera's field of vision [99, § 3]. Still the regulations in regard to PuL need to be observed as well.

If the camera will be able to watch a public space then it has to be approved by the local "länsstyrelse" beforehand [99, § 5].

Inside a shop (but not restaurant or similar) cameras may be installed to prevent theft if they can not be panned or zoomed, they only observe the entrance and cash register area and a written agreement has been made with the employees or their representative [99, § 12].

Unless otherwise approved may the recorded material only be kept for topmost one month.

4.2.4 Copyright

The three EU directives have been implemented by amending the existing copyright law ("upphovsrätt" [94]). But unlike in Austria or other countries, the employer also receives the moral rights on the work created by his employees, which allows him further reaching modifications of the work [170, p. 11].

Another important difference from other countries is that there is no right to ones own picture (in German "Recht am eigenen Bild"). The "upphovsrätt" only covers the rights of the author or creator, but does not specify the rights of the person whose picture is taken. This reaches so far as that the hidden filming of a person can not be prosecuted [121]. Only when such personal data is published can PuL, or an act of libel, be applied.

4.2.5 E-commerce and signatures

Sweden has implemented the e-commerce directive in the "Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster" (act about electronic trade and other services of the information society [105]), although with the alteration that a Swedish court or other state entity may disallow a foreign party to conduct e-commerce in case it is necessary to protect

- the public order and safety
- the public health
- consumers

In such a case the EU has to be informed and consulted about the matter.

4.2.5.1 Information requirements

The same requirements as in the directive are given:

- name
- address
- email address

And, if applicable

- organizational number
- tax number
- regulatory agency

4.2.5.2 Spam

The articles about commercial communication [8, art. 6-7] have not been implemented in the Swedish law as part of the e-commerce legislation. Instead the marketing law ("marknadsföringslag" [109]) has been amended to include email and other forms of electronic communication as further means of advertizing to an individual. Article 5 of the directive [8, art. 5] about information requirements is covered in [109, § 12] of the marketing law, but with modifications:

- The properties of the product have to be described in a way that is adequate for the media in use and the product [109, § 12 lit. 1].
- The sender has to reveal his "identity" [109, § 12 lit. 3], but it is not further specified what details are meant by this.
- Apart from the pricing and delivery details also the process of how complaints will be handled has to be included, if they differ from common trade conventions [109, § 12 lit. 4].

Unsolicited communications ("spam") are not allowed to be sent to physical persons without prior consent [109, § 19], which means that Sweden uses an opt-in system. Consent can be assumed if the recipient has

- provided his electronic address during the sale of a product, and
- not denied the usage of his electronic address for this, and
- the content is about similar products of the same provider, and
- an easy and cost free possibility to stop the usage is provided to the recipient as part of each message.

Furthermore every message, even such to legal entities, has to include a valid response address to which requests for removal can be sent [109, § 20].

If a vendor from within Sweden [109, § 22 lit. 2] offers some kind of guarantee for the product, then he has to include informations about it and the customers requirements to claim it.

The consumers agency ("Konsumentverket" [152]) can be applied to if a consumer wants to take action against unsolicited communications or other forms of illegal business behavior.

4.2.5.3 Hyperlinks

There exists no specific legislation in Sweden in regard to hyperlinks. In the past years only two relevant court decisions have been made where linking had been an issue. In general the linking party is not responsible for the content that it links to, unless it uses the target content within its own (business) context [119]. The latter is the case, for example, if a merchant puts a link next to his product which links to the product description on the manufacturer's website.

4.2.5.4 Signatures

Sweden has implemented the directive in the "Lag (2000:832) om kvalificerade elektroniska signaturer" (act about qualified electronic signatures)[102] and the "Förordning (2000:833) om kvalificerade elektroniska signaturer" (ordinance about qualified electronic signatures [103]). The Swedish law is a nearly literal implementation of the EU text, with no significant changes.

Electronic signatures have been widely used in Sweden before other countries. In 2001 the major Swedish banks formed a consortium [143] to provide signatures to their customers and shortly afterwards the government started to provide them as well [150] through the national personal ID cards. Today it is very common to do online banking and administrative applications over the Internet by using those methods.

4.2.5.5 Electronic bulletin boards

A lot of communication on the Internet is done through public readable forums or similar mechanisms. Sweden has therefore implemented a specific law [98] for such environments which applies unless

- the messages are only exchanged for technical purposes, or
- the forum is used exclusively within the government, a company or a group of companies, or
- the forum is protected by the freedom of speech, or
- the recipient is a specific person or group of persons.

The provider of a forum is required to

- inform any participant upfront about how messages will be visible to other participants [98, § 3], and
- monitor the forum within a reasonable effort [98, § 4], and
- remove any illegal content as soon as he becomes aware of it [98, § 5].

4.2.6 Electronic communications networks

Similar to the situation in Austria may a party that provides wireless network access to the public be considered a provider under the "Lag (2003:389) om elektronisk kommunikation" (act about electronic communication [106]). The Swedish implementation of the intellectual property directive (IPRED [22]), which amended the copyright law [94], then imposes the obligation onto him to provide any party who sues for copyright infringement with the personal details of his client.

In practice this is often not relevant, since the law only requires to provide existing data. Some Internet service providers therefore stopped to store log files or other traffic related information about their customers to avoid those obligations [142]. It also has to be noted that Sweden has not yet implemented the data retention directive [25], which means that this practice is not against the law.

4.3 Local court decisions

4.3.1 Publishing of personal information on a web page

4.3.1.1 Journalistic purpose [114]

Although this incident happened in 1997 and the court decision was made in 2001, it still has influence on the current application of PuL.

In this case the owner of a Swedish web page ("Foundation against Nordbanken") published personal data about several top managers of Nordbanken, a Swedish bank, out of anger about the current banking crisis in Sweden. The published information included lots of personal data, such as suspicions by the police that this person is involved in a crime, but also personal comments from the owner about the managers. Furthermore it allowed the users to add more information and link it to other public data. This seemed of course to be in breach with the "datalagen" (data act), the predecessor of PuL; also it seemed to be a structured database that has not been registered with Datainspektionen.

His defense was that he offered the data in a way that is not automatically processable and which is meant for journalistic purposes. He brought up further proof that his site indeed did research and was meant to inform the public, and also that the data was collected from public sources. Therefore it needs to be protected as freedom of speech under the PuL clause, which came into action 1998.

The supreme court decided in the end that the web page indeed was intended to inform the public, although in a very subjective way, and therefore is protected under freedom of speech. The indictment was therefore dismissed.

4.3.1.2 Private homepage [117]

An employee of a local church made, after taking part in a web page design class, a homepage with general personal information (names etc.) about her co-workers, but also included one piece of medical information ("has a broken leg").

The court decided in this case that the compilation of a list of people on a web page indeed constitutes a structured database according to PuL, which here even included sensitive data. Although the personal data was of rather public origin, she would still have needed to apply to Datainspektionen beforehand.

Although the court found her guilty of breaking PuL, it was in this case (for various reasons) considered a minor contravention and the case was dismissed.

4.3.2 Publishing on a web page equals to export to a third country [120]

The Lundberg's Foundation School published on their web page personal data about one employee by stating that he had difficulties with teamwork and was on sick leave. Apart from the obvious PuL violation the court ruled furthermore:

- Any information published on a web page has to be considered as transferred into a third country, since the web page is visible worldwide. This was also confirmed in other court decisions [117].
- The chairman of the school, who actually manages the homepage, was also appointed by the school to do this task. Therefore it is his responsibility to comply with the law, which means that he will have to bear the sentence, in this case SEK 40.000.

4.3.3 Publishing under a false name [116]

A man created several ads on the Internet under the identity of his former partner, claiming that she was looking for sexual contacts. He included personal data about her, but according to him not sufficient enough to identify her, and also a photo that was supposed to depict her (although it did not).

The court ruled that the provided data was detailed enough to identify her. Also the picture must have been perceived by the viewer as depicting the victim, no matter if it was really her or not. Since the ad was available to more than 900.000 viewers according to the webmaster of the site, the court saw this as a severe breach of the victim's privacy and therefore convicted the accused to three months in prison and a fine of SEK 100.000.

4.3.4 Access to public information

In all of the three following cases the court assumed that the requesting company will treat the data in question internally according to PuL, the part that shall be discussed here is whether the company should get access to the data in the first place.

4.3.4.1 University records [112]

A private company requested from KTH, a public university, the names, grades and addresses of all students who finished during the last four years (ca. 1.400 records). It intended to use this for recruiting purposes and requested the information under the Swedish publicity principle. KTH denied this request by claiming that the information is protected under PuL and that the company has not been registered to operate such a database.

The company argued in court that it requests the data only sorted by last name and in paper form, which means that is only searchable by one term and therefore not covered by PuL. Afterwards they intend to manually calculate the average grading and only keep the records of those students above a certain average score, again on paper and ordered by this score. Those students will then be contacted by phone. At no point will the data be processed electronically.

The court followed this argumentation and the data had to be disclosed.

4.3.4.2 Recipients of student loans [115]

Sweden has a central register of student loans, issued by the state, from which a company wanted to have the name, address and email address of the students. It intended to send them once per term an offer for a student discount card. The request was denied based on privacy considerations.

Since the offer was only to be sent once every six months and the recipients could opt-out at all, the court decided that the information had to be disclosed. The commercial interest of the company outweighted in this case the privacy interests of the students, since the students could benefit from the offer. Furthermore it was stated that although being on the loan list implies that the student does not have lots of money, it does not allow any further deductions about his financial situation and therefore this data is not considered sensitive.

4.3.4.3 Farmers records [113]

A producer of farming supplies asked the ministry of agriculture for a copy of the milk farmers register, which includes their name, address and milk quota. The ministry denied the request based on privacy concerns.

The Supreme Court ruled that the register has to be disclosed, based on the considerations that the commercial interest of the producer outweights the privacy interests of the milk farmers, who in this case have to be considered professionals and not private persons. Also the farmers will have the opportunity to opt-out of any marketing material they might receive [109, § 20].

4.3.5 Publishing of the bankruptcy index [125]

After a finance company went bankrupt a professional liquidator, another company, was assigned to the task. As part of their work they published the bankruptcy estate list on the Internet, which included the names of all debtors and creditors and their respective amounts. They argued that this list is public anyways since everybody can get it from a government agency as well and also that every creditor has the legal right to see the information about other creditors, and therefore it is not protected under PuL.

The court ruled against this, stating that the creditor and debtor amounts have to be considered sensitive data. The fact that the information is available to the public by the government does not imply the right for a third party to publish it. Instead they would have to obtain the written consent of any affected person, as mandated under PuL.

4.3.6 Website protection under the "utgivningsbevis" [124]

On a website, which had an "utgivningsbevis", several blogs were hosted. One of them posted an email and IP address and asked its readers to find out who is behind them, which they did by posting it in the comments section.

The Office of the Chancellor of Justice decided in this case that the blog post itself was protected under the freedom of speech act, but the comments were not, since they were not under the control of the editor.

4.3.7 A juristic person is not protected by PuL [118]

A company did not receive its tax statements from the government due to a wrong address record at the government agency and therefore didn't pay their taxes, which lead to an execution title. The company claimed that, according to PuL, the government was obliged to correct the data based on other correspondence that the two exchanged.

As part of this case, which is more complex, the court stated that a juristic person is not covered by PuL and the company therefore had to explicitly inform about the new address.

4.3.8 Fingerprint database not allowed for minor identification usage [122]

In this case a school used a fingerprint system to identify which pupils may get a meal from an automated system, based on if they have pre-paid it. The registration and usage of the fingerprints was done without written consent, since the school argued that only 30 data points of the finger are scanned, which is not equal to a full print, and that the computer system is independent from other school databases. It is therefore not sensitive data, just private one, and since the interest of the school to serve meals only to paying customers outweights any privacy considerations, the processing should be allowed.

The court ruled against this, citing that any biometric data, even if it is just 30 data points of the finger print, already constitutes sensitive data. Furthermore the school can use less intrusive methods to authenticate their customers, such as food stamps or magnetic cards. For both reasons the written consent of the pupils or their parents is required.

4.3.9 Missing product information [123]

A car evaluation company offered through its website a service to determine the value of the customer's car and send the result back to him via SMS. Due to the misleading design of the website the customers were often not aware that they will be charged SEK 399 for this service. There was also just a small note in the fine print about their rights to cancel the contract under the distant marketing law. Furthermore the company claimed that, since the evaluation of the car started at once, they already have waived this right. Last, the terms and conditions of the contract were only available on the web page in fine print, since the company claimed that this page has to be considered permanent and therefore fulfills the information duties under the law.

The court dismissed all claims by the company and stated that the information in fine print was not sufficient to inform the customers. Since the pricing was not very visible while the customer enters his contact information, it was not sufficient either. The court stated that the information has to be displayed in a way which is consistent with the Internet as a communications medium. The company also has to include the informations according to [107, § 7] in the sent SMS, since this is the only confirmation which the customer will receive.

4.3.10 Responsibility for linked web pages

4.3.10.1 Links to MP3 files [111]

In this case from 2000 a private person put links to MP3 files on his homepage. The files contained unlicensed music, but were hosted on a server outside Sweden which had no relation with the defendant. He claimed that he put the links only there to attract more visitors for his homepage.

The Supreme Court ruled that, apart from the question if the files were legal or not, the linking party is not responsible for their content since the other server was not under his control.

4.3.10.2 Links to pages which infringe copyright [119]

The accused company is part of larger enterprise with branches in various countries. The name of one of their products contains a term to which the plaintiff holds the copyright in Sweden. Although the company was not actively using this term, it was still part of their product descriptions which are hosted by the enterprise in Denmark. The defendant argued that, although their web page was linking to those descriptions, they had no control over the Danish sister company, and therefore can't be held responsible.

Here the court ruled that although the defendant only links to the pages they still use them for their business purposes and to describe their own products. The defendant is therefore responsible for the linked content and in this case is guilty of copyright infringement.

4.4 Guidelines and decisions made by Datainspektionen

4.4.1 Guidelines

A lot of disputes are directly settled by Datainspektionen and therefore never taken to court. From their experience with this work they have published general guidelines [147] for common issues, from which some examples shall be discussed here.

4.4.1.1 Entrance and exit log

Instead of relying on the personal reports of their employees a company wants to install an electronic gate to monitor their working hours.

Since this kind of control can be done with less intrusive means the company may only use the electronic gate if specific evidence indicates that misuse is happening. In any case is it required to inform the employees about what kind of data is collected and for which purpose.

4.4.1.2 Usage of photograph in employee database

A multinational company wants to include a picture of their employees in their company-wide human resources database, which can only be access by a small group of people.

Since the privacy interests of the employees are higher than the unsubstantiated reasons of the company, the explicit consent of the employees is required. It is also required to allow the transfer or making available of these pictures outside the EU or equal areas.

4.4.1.3 Mobile phone cost controlling

A company allowed private calls on their business mobile phones, as long as the costs don't become a financial burden. To control this they started to evaluate the bills and call lists on a per phone base. This is allowed since the company has provided the phones for a specific task and may monitor if the usage is in compliance.

4.4.1.4 Video surveillance of the server room

Assuming that the data will not be linked to a structured database, the privacy of the server operators has to be considered against the interest of the company to protect its assets. A general answer can therefore not be given.

4.4.1.5 GPS tracking off-site employees

If the information is used to keep track of vehicles and calculate their mileage, then it may be done with prior consent of the drivers.

In other cases it has to be in accordance with the purpose of the company, the interest of the company has to be higher than the employees' and they have to give their consent. In any case it may not be used to control working hours since less intrusive methods are available.

4.4.1.6 IP phones

Since the information is usually only transported in this case, PuL is mostly not applicable here. The only exception is that malicious code or other parties might intercept the conversation; according to PuL it is therefore necessary to provide sufficient technical protection for the transport.

In case one of the parties wants to record the conversation or if logging information is to be processed or stored, PuL has to be fully applied.

4.4.1.7 Monitoring of emails and Internet usage

According to PuL may any personal data only be used for a specific purpose, minimal required time and with the least required amount of data. The employer therefore needs to publish rules about what kind of data is being collected and for which purpose. Furthermore the terms "misuse" or "misconduct" need to be defined so that every employee clearly understands what he may or may not do with the IT systems and under which circumstances his traffic might be monitored.

Nevertheless, if the company allows private usage, of for example emails, they may not inspect this private information. It is therefore required that guidelines are made available about how to separate this private information from the company one.

4.4.2 Decisions

Apart from event driven investigations, Datainspektionen mostly does routinely inspections of public entities and publishes their findings or recommendations. Since PuL applies to those institutions and private companies in the same way, the results can also be used there.

4.4.2.1 Usage of social media

Some agencies use Facebook ([138], [139], [140]) or similar pages to publish information about themselves and to answer questions. It furthermore allows their users, in case of Facebook their “followers”, to post their own messages on this site. Since the owner of the page, the government agency, can configure what services are available to the public, they are not only the data processor for their own data according to PuL but also responsible for the informations published by other users.

Datainspektionen argues, that it is the free decision of the page owner to allow comments, therefore they also have to take the responsibility for them in case personal related data is published. However this does not required the agency to permanently monitor the comments, rather it has to publish guidelines about acceptable content, and remove inappropriate content as soon as they become aware of it. In the case of for example Twitter, the page owner can not control the content (“tweets”) that other parties send him, therefore they can not be held accountable for it.

4.4.2.2 Unmoderated forum

A Swedish website offered its users to review local companies, either the ones automatically added through queries of public databases or by adding a new entry through a user. The site claimed that it is not responsible for the published data since it only provides an unmoderated forum and requires the users through its terms and conditions to obey PuL and other laws; therefore the users are in fact the data processors.

Datainspektionen rejected this argument [136]. Since the site owners designed the functionality and also have the possibility to edit or delete comments, they are in fact responsible for the published personal data.

The site also claimed that, since the data is about companies, it is not protected as personal data. This was in part denied by Datainspektionen, since they also had data about small businesses that trade under the owners name, which therefore is personal related data [97, p. 341].

4.4.2.3 Access to personal data

A private company offered in their web order form for customers the functionality to enter their personal number ("personnummer") and then have their address information automatically filled in. This was done by the web page through a web service offered to companies by the central registration office, a government agency.

Since this could be done before the order was completed, it could be misused to retrieve the address information of any (unprotected) Swedish citizen if their personal number was known.

Although those informations are public in Sweden, Datainspektionen ordered [137] the company to remove this function since it is not a core requirement of their business. The privacy rights of their customers are more important in this case than the desire of the company to simplify the order process.

4.4.2.4 Video surveillance

A local bus operator had problems with sabotage and the distribution of hate speech pamphlets within its bus depot, which is only accessible by employees. The company therefore installed hidden cameras to investigate.

After this became public, Datainspektionen filed a complaint [133] since this is in breach with the video surveillance law and PuL, especially since one of the cameras also was aimed at the entrance of a workers union space. It is clearly stated that only law enforcement agencies might use hidden surveillance whereas a public company has to inform the affected people upfront about it.

In another case [134] a shop owner installed four hidden cameras in the back office, in addition to several visible ones inside the shop and one outside. Datainspektionen decided that, for the same reasons as above, the hidden cameras are illegal. Also the camera in front of the shop was an intrusion into the privacy of bypassers and had to be removed. Furthermore had the shop owner the ability to watch all those cameras from home over the Internet. This was considered unnecessary for the stated purpose, namely protection against robbery or theft, and therefore also had to be removed.

4.4.2.5 Utgivningsbevis

A public school published regularly information about their internal proceedings and decisions, which in one case included the names of two pupils who were extolled from the school. The school argued that, since they own a publishing certificate ("utgivningsbevis"), PuL can not be applied in this case.

Datainspektionen, in line with the Federal Court, has decided that this publication is not protected and PuL is applicable. The only reason for this decision is that the public school is part of the government and therefore can not claim the protection of freedom of speech.

4.4.2.6 Required authentification method

The Swedish National Service Organization ("Pliktverket", the military recruiting agency) provided a web interface where all examined people could log in and access their medical records and other personal data. The authentication was done through the personal number ("personnummer") and a pin code, which was sent by regular mail.

Since this is highly sensitive medical data, Datainspektionen decided that a simple eight digit pin code does not provide sufficient protection [132].

Also the information, required by PuL, about the data usage is found under the "about us" link on the web page, but not directly on the pages with the personal data or the login page, which Datainspektionen therefore considered insufficient.

4.4.2.7 Keeping of old business data

A travel company stores its customer data within a customer relationship management (CRM) system, which includes contact data, travel details and information about complaints. If the customer does not book another travel within three years then the data is removed from the CRM system, but will still be kept in an archive for 10 years due to accounting laws.

Datainspektionen remarked [130] that the data should only be kept for two years, as common in the travel business. For longer periods the consent of the customers is required. Also it has to be investigated what parts of the customer data need to be archived for accounting, some details such as complaint letters might not be necessary and therefore should be removed.

4.4.2.8 Customer data

One of the largest grocery chains in Sweden introduced a discount card program to provide its customers with special offers for products they often buy. This was done through a database of all the items that were bought by each customer. Although the customers who used the card could opt out of the advertising, their shopping lists would still be recorded.

After a four year monitoring period this was found to be according to the law by Datainspektionen [131]. Every person who signs up for the discount card is informed in a proper manner about the way the data will be collected and for which purpose it will be used, and they have to give their consent by signing the application.

4.4.2.9 Encrypted transmission

The social service of a city offered help for various health and social related questions via its website. The users could send in an email and the team would respond by publishing the information anonymized on their web page, or directly by email if requested.

Since this involves a lot of sensitive information, Datainspektionen ruled [128] that the response email has to be encrypted so that only the intended recipient may read it, especially since it is sent through the public Internet.

In another case [129] used a public school a web platform where the parents could enter information about the absence of their children, such as sickness or a doctor's visit, and the teacher could then see this information. The access was protected by a username and password, which was sent to the parents by email.

Again Datainspektionen ruled that since this involves sensitive data, the access had to be protected with stronger mechanisms such as the Swedish "e-legitimation". Furthermore the email to the parents needs to be encrypted as well, so that only the intended recipient may read it.

4.4.2.10 Processing of criminal records

A USA based consulting company that operates worldwide is by USA law required to register with the SEC (US Securities and Exchange Commission). This includes in depth information about their business processes and also informations about their employees, such as if they have been convicted to more than one year of prison for breaking a law.

The company applied to Datainspektionen for an exception from PuL, so that they can collect and process this information from their Swedish employees. They would like to ask them three simple yes/no questions, so no full criminal record would be used.

Datainspektionen denied the request [127] since the general questioning of all employees is a too deep intrusion into their private life and is not outweighted by the business interest of the company.

In a second case the local traffic operator for Stockholm (SL, "Storstockholms lokaltrafik") wanted to combat their graffiti problem by creating a database with information about each incident, such as a picture, the "tag" (nickname of the graffiti creator or group), time, place and the police register number. They argued that this would allow them to correlate individual incidents, for example through the "tag", and therefore aid the police in finding the offender.

Here Datainspektionen noted that the "tag" might also be personal information, since it can be related to an individual and that in this special case the whole content of the database is basically visible to the public, since SL is a state owned company and therefore has to observe the "offentlighetsprincip". Still, the interest of the company to reduce their damage losses has to be seen higher than that of the offenders, and therefore the exemption was approved [126].

Chapter 5
A comparison of Austria and Sweden

Both countries implemented the directive in mostly the same way in regard to its structure and intention. In the following shall the differences between each other or to the directive be discussed. Terms or mechanisms which are identically between the two countries and the directive are not further investigated here.

5.1 Legal environment

Although at first glance both countries seem to be similar in regard to population size and economy, distinct differences can be seen in the legal area and in the way how the Internet is used in daily life.

5.1.1 The legal entities

The Austrian administration is organized in a very hierarchical way, with a minister on top of each department who is authorized to issue instructions down to each level.

In Sweden the government departments are rather small in size. The actual daily work is done in independent agencies (“myndigheter”), which only execute the laws without the possibility for the minister to directly influence them.

Also the general public in Austria perceives a ministry more like a supervising body, sometimes even an annoyance. The Swedish public, on the other hand, sees their “myndigheter” more like service providers which are there to help them, sometimes even owe them a service.

As a result of those general philosophies the implementation of the independent governing agency, as required by the EU data privacy directive [3], differs greatly.

Austria implemented the DSK like any other agency, thereby utilizing state personal, which makes it in practice very dependent on the government. This had the effect that the public saw a need for an independent party, and thus ARGE Daten was created as a counterpart. Furthermore the DSK is provided with only very limited resources, and can therefore only exercise basic duties. A lot of investigations, training and law suits about privacy violations are therefore done by ARGE Daten, a private society with its own agenda.

The Swedish Datainspektionen is in practice independent and also has sufficient funds for their duties. A lot of their work involves interactions with other state agencies to solve data issues. But they also investigate private companies, respond to complaints from citizens and provide training. It can be said that Datainspektionen is well integrated into the Swedish society and the state administration.

5.1.2 Data protection philosophy

In Austria any personal related data is considered to be part or property of that person and can therefore only be utilized with his agreement. Very strict boundaries are set in how this data might be used and by whom. It is in general rather uncommon to share personal data with the public or for the government to provide internal data to citizens ("Amtsverschwiegenheit", official secrecy).

Sweden, on the other hand, has a long history of providing certain personal data to the public. The public principle ("offentlighetsprincipen") allows any citizen full access to government records, even those about other citizens, such as their tax records. Still, data misuse is absolutely not accepted by the public. The general idea is that a specific data set is provided to a specific party for a very specific purpose, because that party is providing a service. If that party happens to be a government agency, then anybody should have access to it since the government, in the end, is a servant of the public. The question of privacy is therefore not a black and white decision, but rather shades of gray, which can be observed in a lot of court decisions where the interest of a third party is weighed up against the privacy of the data owner.

5.1.3 Daily usage of personal related data

Although Austria is already using electronic data exchange heavily within the state administration, it is rather uncommon between the state and private or commercial parties. The biggest hindrance is probably the lack of a widely available public key or certificate infrastructure. The introduction of the “Bürgerkarte” [84], a chip card with a signature, has so far had a very bad reception and the card is not in wide use, especially since it requires a card reader device. Electronic signatures between companies only exist as isolated applications, and between companies and private parties basically only for electronic banking.

In Sweden the first electronic signatures were introduced by the banking sector. It included the possibility to download the certificate into the browser, which was perceived as secure since the user also had to authenticate to his banking application via a hardware token. This service was therefore already in widespread use when the government introduced their online services, which lead to a good acceptance by the public. Today a certificate can be obtained either through ones bank or from the Ministry of Finance. It is very common to interact with state agencies through secured web services or for private parties to do business over the Internet.

5.2 Adaption of the EU legislation

5.2.1 Implementation of the directives

Both countries have implemented all relevant EU directives in national law with the only exception that Sweden has not yet adapted the data retention directive. There are still debates ongoing about how this will have an impact on the freedom of speech and how it may be compatible with existing laws.

5.2.2 Definitions

5.2.2.1 Official translation of the directive, as provided by the EU

English	German	Swedish
personal data	personenbezogene Daten	personuppgifter
processing	Verarbeitung	behandling
filing system	Datei	register
controller	für die Verarbeitung Verantwortlicher	registeransvarig
processor	Auftragsverarbeiter	registerförare
third party	Dritte	tredje man
recipient	Empfänger	mottagare
the data subject's consent	Einwilligung der betroffenen Person	den registrerades samtycke

Table 5.1 Official translation of the directive

5.2.2.2 Wording of the implementations

EU / English	Austria	Sweden
personal data	personenbezogene Daten	personuppgifter
indirect person related data	indirekt personenbezogene Daten	-
especially protection worthy data	besonders schutzwürdige Daten	-
affected person	Betroffener	den registrerade
data application	Datenanwendung	-
data collection	-	samling
filing system	Datei	-
usage	verwenden	-
processing	verarbeiten	behandling
blocking (of a transfer)	-	blockering
cede	überlassen	-
transfer	übermitteln	överföring
controller	Auftraggeber	personuppgiftsansvarig
assistant (employee) of the controller	-	personuppgiftsbiträde
data protection officer (of the controller)	-	personuppgiftsombud
processor	Dienstleister	personuppgiftsbiträde
interconnected information processing system	Informations-verbundsystem	-
branch office	Niederlassung	-
representative	-	företrädare
third party	Dritte	tredje man
recipient	Empfänger	mottagare
the data subject's consent	Zustimmung	samtycke

Table 5.2 Wording of the implementations

5.2.2.3 Person or data subject

The directive clearly states that the data of natural persons shall be protected ("an identified or identifiable natural person" [3, art. 2 lit. a]), which Sweden implemented as "en fysisk person som är i livet" [100, § 3] ("a living physical person").

Austria, on the other hand, extended the coverage by stating "natürliche oder juristische Person oder Personengemeinschaft" [31, § 4 lit. 3] ("natural or legal person or association of persons"), which thereby also covers companies or other legal forms.

The practical effect is that in Austria for example any customer database about companies has the same level of protection as one about single persons. The consent of a company is therefore needed if one would like to process their contact data or similar.

5.2.2.4 Personal data

The terms "specially protectable data" and "indirect personal data" have been implemented in the same way, but Austria also introduced two more terms.

The first, such as criminal convictions or credit scores, are covered in Sweden as "personal related data", such as anything else that is not specifically "sensitive data".

Indirect data is not known in Sweden, since it is always looked at if the processor can relate the data to a person, even with the aid of a third party that might be available for him. If there is no way to relate it, then it is not considered personal data.

5.2.2.5 Personal data filing system

The directive describes such a system as a set of personal data "which are accessible according to specific criteria" [3, art. 2 lit. c]. This has been translated into German as "die nach bestimmten Kriterien zugänglich sind" and into Swedish as "som är tillgänglig enligt särskilda kriterier".

Although all three versions use the plural of criterion, which would indicate two or more, Austria has implemented this as "die nach mindestens einem Suchkriterium zugänglich sind" [31, § 4 lit. 6] ("which are accessible by at least one search criterium").

As a result of this any sorted data collection, thereby accessible by at least one criterion, is protected in Austria, whereas it would not be in Sweden, where it needs to be accessible by at least two criteria.

This has practical implications especially for sorted paper filings, since those are usually sorted by exactly one criterion.

5.2.2.6 The data subject's consent

The Austrian law requires that the data subject is aware of the circumstances when he gives his consent ("in Kenntnis der Sachlage" [31, § 4 lit. 14]), whereas the Swedish law requires that he had been informed up front ("efter att ha fått information" [100, § 3]).

While this is a subtle, but relevant difference, in such as that the Swedish law requires an actual information transfer to the data subject, no court decision or other incident could be found to elaborate this further.

5.2.3 Legitimation

While the basic requirements [3, art. 6] are implemented nearly literally in both countries, the "Criteria for making data processing legitimate" [3, art. 7] differs.

Sweden basically just translated the text into Swedish [100, § 10], while Austria crafted a more complex system in the DSG.

The term "schutzwürdige Geheimhaltungsinteressen" (privacy interest which is protection worthy) is introduced in [31, § 7]. It is then defined under which circumstances those are not violated, in [31, § 8] for non sensitive data and in [31, § 9] for sensitive data. Also several cases where the interests of a third party prevail are explicitly defined for both kind of data, such as:

- to fulfill vitally important interest of a third party
- to protect claims of the processor in court
- in case of a catastrophe to identify missing people or find their relatives

The Swedish personal number is a special case [100, § 22], where the processing is allowed without explicit consent if an unambiguous identification is required. In practice this is handled rather restrictive by Datainspektionen when it comes to IT systems [146], since using individual usernames fulfills the same purpose without disclosing personal information.

5.2.4 Information duties

Both countries have extended the directive in this regard, Austria even in a very detailed way.

Both allow one data inquiry to a controller per year free of charges. While the request in Austria has to be done in written and by proving ones identity, which would allow the usage of digital signatures, Sweden requires a written and (hand-)signed document, which in practices means a letter. The reply has to be given in Sweden within one month and in Austria within eight weeks, or can be denied in both countries if the required effort would be disproportional high.

Sweden has no regulations in PuL about exceptions [3, art. 13] due to national security etc., since those are handled by the "offentlighetsprincip" [110].

Austria also added that the controller may not delete data about a person for four months, beginning from the notification about an inquiry [31, § 26 art. 7].

5.2.5 Correction and removal duties

The directive grants every person the right to demand rectification, erase or blocking of his data [3, art. 12 lit. b].

This was implemented in Austria as the right to demand the data to be deleted or to be corrected, both within eight weeks. The term “blocking” is not used in the DSG.

In Sweden the decision about the action to be taken is done by the controller [100, § 28]. The idea behind this is that the controller has to make sure that his usage of the data is according to the law, how he does it is up to him.

All of those rights, information, correction and removal, can not be utilized in Austria if the controller only uses indirect person related data [31, § 29].

5.2.6 Confidentiality and security

Sweden has rather simplified [3, art. 17 lit. 1] in that the controller is only required to protect the data by adequate means, but not specifying which threats he has to protect against [100, § 31 art. 1]. On the other hand specifies PuL that, if a subcontractor is used, the controller not only has to check if he is able to provide the necessary security measures but also that he really utilizes them [100, § 31 art. 2].

Austria added a lot of detailed instructions to their implementation, which do not exist in the Swedish PuL:

- Every employee has to be instructed about his duties according to the DSK.
- All processing orders for employees need to be kept in a way so that they can inform themselves at any time.
- All employees need to be bound by a contract that allows them to use personal data only according to processing orders and that they have to keep it secret even after leaving the company. Subcontractors may only use employees that are also bound by such a contract.
- The access controls to the company rooms have to be defined.
- The logical and physical access controls to software and data has to be defined.
- The access to computers with personal data has to be protected.
- Any access to personal data has to be logged, but this logs may not be used for other purposes, such as performance reports about employees.
- All organizational measures to accomplish this need to be documented. Both this and the log files have to be kept for three years.

An Austrian subcontractor may only utilize further subcontractors if he informs the controller about this up front and he agrees [31, §11 art. 2 lit. 3]. The Swedish implementation does not have such a restriction.

5.2.7 Registration and notification

Very different approaches have been used in this case by the two countries.

Austria did not implement the data protection officer [3, art. 18 lit. 2] and therefore requires the registration of every database or application that uses personal data. The registration has to be done electronically with a digital signature, which in practice means using the "Bürgerkarte". The only exceptions are standard applications, as defined in [40]. But since most of them aim at the public sector and the remaining ones often don't cover all the data items utilized by companies, those exceptions quite often can't be taken into account. A documentation about the security measurements according to [31, § 14] also has to be included. If sensitive data is included then a prior assessment by the DSK is required.

Sweden tries to shift the responsibility more to the controller. In general needs every data application to be registered, but there are several exceptions as described before 4.2.2.1, which in practice means that only uncommon applications, and such about sensitive data, will have to be registered with Datainspektionen. If a registration is required, then it has to be done in written and signed by the controller since an electronic registration is not possible.

In comparison it can be said that Austria tries to have a central register of all applications, whereas Sweden strives to make sure that somebody, preferable one close the the application, is always responsible for the data usage and can act as a contact person.

5.2.8 Transfers to third countries

Both countries allow the transfer and processing within other EU members, as well as in the USA if the recipient has signed the "Safe Harbor" agreement, and into countries with an adequate level of protection. The latter cases are in Austria defined by the chancellor [31, § 12 art. 2], in Sweden by Datainspektionen [100, § 35 art. 3] or in general through EU regulations:

- EU
  - Argentina
  - Guernsey
  - The Isle of Man

  - Jersey
  - Switzerland
  - Canada (under certain circumstances)

- Austria [30]
  - Switzerland
  - Hungary
- Sweden [148]
  - Norway
  - Iceland
  - Liechtenstein

It can be seen that both added those neighboring countries which at that time haven't been EU members (Hungary joined in 2004, but the Austrian act is from 2002). Sweden chose the option to simply include all European Economic Area members to achieve this.

5.2.8.1 Other countries

Unless covered by the exemptions in [31, § 12], Austria requires a pre-approval from the DSK and a legally binding agreement with the foreign party before personal data may be transferred. One such exemption is found in [31, § 12 art. 3 lit. 2], which allows the transfer if the data is only indirect personal related for the foreign party. This opens the possibility to pseudo-anonymize the data before the transfer and then recombine it when the results come back. Before mentioned agreements are specifically the EU standard contract clauses [13] or Binding Corporate Rules (BCR), or other contracts if approved by the DSK.

Sweden also allows the transfer if such contracts are used [101, § 13 art. 2], but does not require any approval in such a case.

5.2.9 Penalties

The EU directive only defines that a victim is eligible to remedies [3, art. 22] and that the controller can be held responsible in such a case [3, art. 23], but does not give further details.

The Austrian DSG defines the punishments in [31, §§ 51-52]:

- Any data misuse motivated to gain profit: up to one year in prison.
- Other misuse of data, as well as denying a court decision to the right to data inquiries, correction or removal: up to EUR 25.000.

- Failure to register an application, failure to get approval from the DSK failure to publish required information: up to EUR 10.000.
- Failure to fulfill a data inquiry, correction or removal request in time: EUR 500.

The Swedish PuL defines in [100, § 49] a prison sentence of up to six months, or in severe cases up to two years, for:

- Supplying false information to a person or Datainspektionen as a response to an inquiry.
- Processing data without a legal base.
- Transferring data to a third country without a legal base.

It should be observed that in Austria the controller, as a legal entity is accountable, whereas in Sweden the physical person, who was responsible for the action, will be held accountable.

5.3 A comparison of practical applications

5.3.1 Video surveillance

As a general idea considers Austria this topic to be related to data privacy, with links to other laws, and therefore included it in the DSG, managed by the DSK. Sweden took the approach that this is about surveillance and protection from crimes, with some links to data privacy, and therefore made a separate law that is managed by the local county administration ("länsstyrelse"). This also leads to the effect that Austria differentiates between analog, digital, live and recorded monitoring, wheres in Sweden it is all considered to be the same, namely surveillance. Only if the data is processed in Sweden in a way that constitutes a database, PuL will be applicable.

Hidden cameras may in Austria only be used by the police for crime prevention, while Sweden also allows them for private controllers upon request [96, § 3].

A significant difference is that Sweden includes audio recordings as part of the video recording, if both are done together, while the Austrian law specifically only allows video images.

Any visible camera needs to be indicated, such as by signs. In Austria it also has to indicate the identity of the controller, if it is not obvious, while in Sweden this is not required if the outside of a building or site is monitored. Also public areas may not be recorded unless it can not be avoided, in which case it has to be kept to a minimum.

Whereas Sweden made an exception that allows monitoring within a shop, which is a common application, in Austria all situations are treated equally.

Austria only allows recordings to be kept for 72 hours, whereas Sweden states up to one month, or longer if applied for.

It can therefore be said that Austria sees video cameras usually as an intrusion into privacy which has to be kept to a minimum, while Sweden rather accepts their usage by providing guidelines.

5.3.2 Internal log file analysis

Both countries have the same position, as mandated by the directive, that log files are collected with a specific purpose, such as securing an IT environment or for technical capacity statistics. Any further analysis, such as employee behavior, is not covered by this purpose and therefore forbidden.

5.3.3 Providing a static web page

A static page is characterized by not allowing any user generated content, although it may publish personal related data.

5.3.3.1 Imprint

Although it is in both countries required to state the identity of the publisher, Austria has far more strict and detailed regulations in this regard. While Sweden follows the idea that the visitor should be able to easily retrieve this information, it leaves the actual layout up to the publisher. Austria however requires the publisher to provide the full information on every page, either directly or behind one link.

5.3.3.2 Logging

The IP addresses of page visitors are considered private data, since they can be related to a person, even if only through a third party. Austria uses the term “indirect personal data” for this, while Sweden considers it personal data at least since the introduction of the IPRED law.

It can still be done in both countries for the purpose of statistics and protection of the page, if the visitor is informed about it. The same is valid for the usage of “cookies”.

5.3.3.3 Publishing personal data

While in Austria personal data can only be published in accordance with the DSG, Sweden adds extensive exclusions through the publishing certificate ("utgivningsbevis"). This can be utilized by private persons as well as companies to claim the "freedom of speech" and therefore circumvent the restrictions implied by PuL.

5.3.4 Providing an interactive web page

In addition to the issues around a static page, the publisher has here to deal with personal information about his users as well as with the content published by them.

5.3.4.1 User list

If a user explicitly has to sign up for a service then his consent can be assumed, and Sweden therefore does not required the registration of the database. Austria has no such exceptions, and therefore it has to be registered, unless it is covered by one of the application templates. In both cases the information can again only be used for the stated purpose.

5.3.4.2 User generated content

This situation arises when a forum functionality is provided, where users can post public visible messages or comment on those of others. Here the owner of the web page has the role of the publisher and the users are the content creators. Problems usually arise if a user publishes offending material but is hidden behind his pseudonym.

In both countries the media publishing laws cover this topic, in Austria [36] and in Sweden [93, 95].

The Austrian law mandates that the publisher has to remove any incriminating content as soon as he becomes aware of it [36, § 6 art. 2 lit. 3a], or otherwise he might be forced to do so [36, § 36a]. The identity of the content creator can be kept secret [36, § 31 art. 1].

Although Sweden provides strong protection through the "utgivningsbevis", this can only be applied to content that is under the publishers control. Forum entries are therefore not protected. Instead the "law about electronic bulletin boards" [98] has to be applied, which includes the same obligations as in Austria, such as removing offending entries as soon as the publisher becomes aware of them.

It is still possible in two ways to utilize the Swedish “utgivningsbevis” for most of the web site:

1. All new forum entries are checked by the publisher before they become visible for others. In this case he has control over the content and is therefore protected by [93].
2. The main web page is separated from the forum page, technically and logically, for example by hosting it on a different DNS name and giving it a different visual layout. In this case the main page can be protected through the “utgivningsbevis”, while [98] only applies to the forum. Using HTML links between those two is not prohibited.

In any case is the publisher responsible for the content, and if legally challenged he will have to defend it.

5.3.5 Publishing of personal information on a web page

In Austria the DSG fully applies, as publishing data on the Internet is the same as making it available to everybody worldwide. No personal related information about employees or third parties can be published without their prior consent.

For Sweden two situations have to be distinguished, depending on the existence of an “utgivningsbevis”. In general the same situation as in Austria exists, in such as that prior consent is required. But with an “utgivningsbevis” PuL can be ignored since the freedom of speech overrules it, and the publishing of personal data can not be challenged in court. Several credit scoring companies in Sweden utilize this to offer complete profiles of every citizen over the Internet, partly even for free and accessible by everyone.

Chapter 6
Summary of the situation in Austria and Sweden

The European data protection directive and its related legislation aims to provide companies as well as private persons with a single set of rules that apply throughout the European Union. But since these need to be translated into national law by each country, certain differences among the member states evolved.

Austria and Sweden have based their laws related to data protection on the same EU directives, but their implementations and legal effects differ. The result is influenced by their existing laws that needed to be adopted, as well as by the general legal philosophy in each country. As a basic principle do both provide the same legal environment for a company, with some different details as described before. The real differences come into effect during the practical application and by looking at how data protection is "lived" in each country.

6.1 Austria

It is safe to say that Austria has a rather strict, detailed legal system that tries to lay out in detail what a citizen may or may not do. Aided by the facts that the DSK is underfunded and that in general not many law cases in regard to data protection are brought to court, it leads to a rather unexplored legal area. The lack of data protection officers further puts more load on the DSK. It also leads to some kind of neglect within the data controllers, since nobody advices them about how to comply with the law or does the actual work there. This is as well noticed by the DSK when they receive applications for data transfers into third countries based on unknown, because unregistered, data applications [47, p. 42].

Austria took they way of implementing the data protection tools as a whole new area of law, which sometimes leads to conflicts with existing legislation. A good example is the area of video surveillance, where Austria differentiates between analog and digital systems, and the question if the material is recorded or not. The decision to implement the supervising agency as an entity that is closely related to the government, thereby acting against the directive, can only be interpreted as an act of unwillingness to "burden" the local economy with the requirements of the directive. The given examples of legal cases also show that the relevant law is seldom applied in practice, and even in such cases it usually involves a government agency as the data processor. Only limited investigation is done by the DSK because of its described limitation in resources.

By looking at the Austrian law in detail it has been shown that the intended purpose of the directive has sometimes been complicated by the introduction of such additional concepts as indirect personal related data or by not implementing a data protection officer. Especially the latter issue leads to considerable costs for businesses.

On the positive side it has to be mentioned that third parties, such as the Chamber of Commerce and ARGE Daten, provide sufficient support for their members to be able to comply with the legislation. For example by providing a company information page on wko.at it is considerably easy for a business to supply all required information according to the e-commerce regulations.

6.2 Sweden

The Swedish law on the other hand tries more to provide a general guideline, which is then enacted in detail through the responsible agency, Datainspektionen. A further level was added by allowing for independent data protection officers within companies, who then can get back to Datainspektionen with questions. This system gives Swedish companies a very interesting incentive to fully comply to the law, by allowing them to handle the registration and monitoring internally through their data protection officers. In cases where the law is broken, complaints to Datainspektionen or law cases are done quite often. It can therefore be said that data protection is a common part in Swedish business life.

Sweden took a slightly different route in implementing the EU legislation by trying to amend existing laws, where possible. This has lead to a good integration into existing legal areas, again for example by looking at the way video surveillance is regulated. The implementation of the governing agency as one of many others also seamlessly integrates with the governmental environment that companies are used to work with. Finally, by encouraging companies to employ an independent data protection officer within their organizations, the majority of the administrative effort is done by the businesses themselves while Datainspektionen can focus on supervising the correct handling of personal information.

The amount and kind of actual court decisions, as well as those handled by Datainspektionen, give an impression that the EU directive is actually used and lived within the Swedish society.

Another success factor can be seen in the interaction of Datainspektionen with the local data protection officers and companies. By providing sufficient information and training courses, while at the same time also doing the auditing, they can ensure the right protection mentality within the companies.

Chapter 7
An IT guideline

In this chapter a guideline shall be given about how to handle IT operations in accordance to data protection and other related laws as discussed before.

The discussion will be done with the focus on the before mentioned categories of data. The terms “business information” or similar expressions are therefore always synonym to “personal related data that is used in a business context”.

7.1 Scenario

The situation of a European company that has business operations in Austria and Sweden will be investigated. Based on the requirements for those two countries recommendations for a general Europe wide operation will be made. The specific situation in each member state will not be looked at, but rather a generic Europe orientated view will be made. This can then in a next step be refined for the legal requirements in each European country.

Since the legal requirements are based on a certain idea of how information should be managed, this guideline will start from the very basics of information processing and then build up a structure that is suitable to comply with EU regulations. While this kind of architecture might not be the only possible one, it has been chosen because it also resembles the current ideas in the IT related sciences.

After the architecture has been defined, practical implementations are described with examples and observations that are relevant to the topic of data protection.

7.2 Overview

As described in the chapters before, the data protection laws can only be fulfilled if a business has an organized IT department. Otherwise it will be impossible to control the usage of personal data, especially its spreading. Further problems will arise when data inquiries need to be answered or corrections need to be done, and it can not be made sure that all record copies are found. Finally, without a well designed and managed IT environment it will be impossible to secure the data storage against loss, or log access to it, both of which are basic legal requirements.

Although this chapter will only have a look at the IT department, it must not be forgotten that the IT and the back office of a company are tightly bound together. When implementing an IT solution as described here, the back office has therefore also to be kept in sync. Usually this is resolved by having, at some point of the hierarchy, the same manager for both departments.

The core layers for an IT department, going from top to bottom, should be

- classification of business data
    - data not related to a person
    - personal data
    - sensitive data
- organizational responsibilities and authorizations
- IT applications and their security concept
- IT services
- physical setup

The reason for this structure is that a company works with data and information in the first place, and the actual executing entities need to be designed according to these needs, not the other way around. Or by using a principle from classical architecture:

> That form ever follows function. This is the law. [168]

Usually it holds true that the smaller the company is, the less organized will this structure be, although very large organizations might also have problems keeping the big picture in sync. Most of the time this stems from a lack of understanding of the benefits, a common argument is that it will lead to bureaucracy and hinders the growth of the business. While this is correct for start-up companies at the very beginning, it has to be taken care of shortly afterwards. Otherwise growth will become chaotic and the back office and IT will spend most of their time on emergency actions instead of supporting the business and optimizing the processes.

Therefore it is mandatory, even for the smallest business, to clearly define the above mentioned areas and keep their IT and process design in shape.

7.3 Systemic holistic view

Before looking at a department in specific, the general and abstract functionality should be investigated. A lot of information is available in the area of management theory, which would go beyond the scope of this thesis. Instead a short introduction and application of Cybernetics, as defined by Schoderbek et al. will be used as the general outline of what management and control is.

7.3.1 Introduction

In their book “Management Systems” [167] Schoderbek et al. defined what kind of systems exists and how their controls work.

7.3.1.1 First-order feedback systems (Automatic goal attainment)

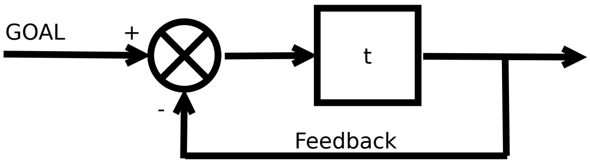

Fig. 7.1 First-order feedback system

Here the output is used as part of the input, so that the system can reach in the end the desired state. The classical example is a thermostat that changes the temperature until the predefined level is reached.

7.3.1.2 Second-order feedback systems (Automatic goal changer)

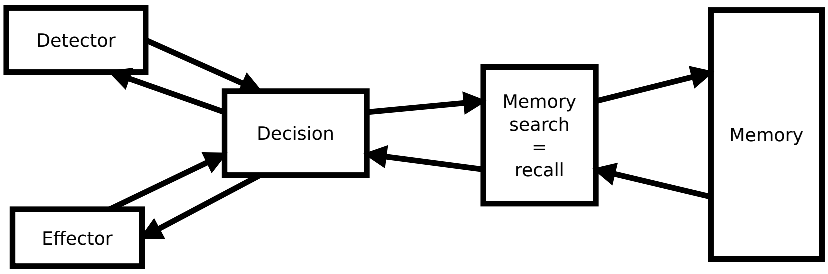

Fig. 7.2 Second-order feedback system

This system has a memory and can react based on past experiences. Expert systems with learning abilities are an example.

7.3.1.3 Third-order feedback systems (Reflective goal changer)

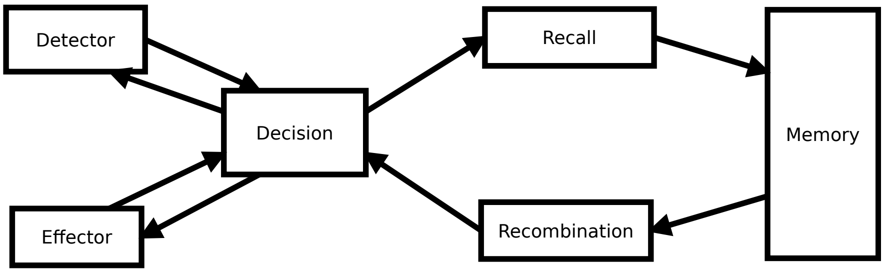

Fig. 7.3 Third-order feedback system (variant A)

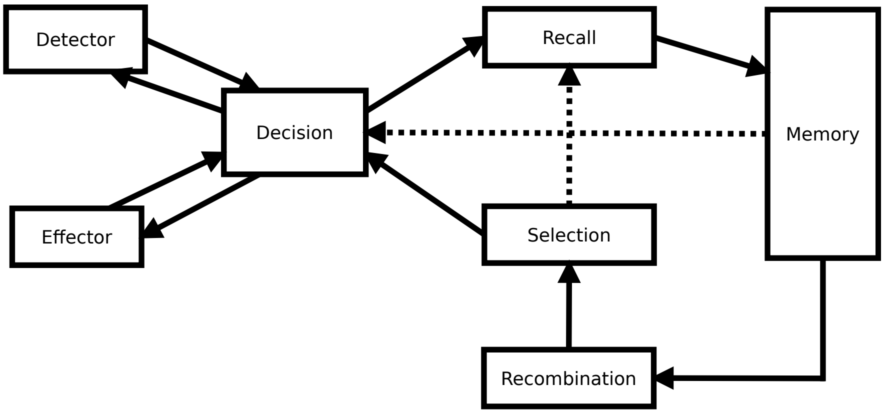

Fig. 7.4 Third-order feedback system (variant B)

Such a system not only has a memory, but can also learn from past decisions and evaluate future action paths to change its decision making process. It is therefore able to reorganizes itself (variant A) or might even develop a kind of consciousness (variant B).

7.3.2 Application in a business environment

Companies are usually considered to be a third-order feedback system, since they are reorganized according to business needs in a permanently changing economical environment.

Unfortunately this doesn't hold true for SMBs in regard to IT security or data protection. Since they often lack the required resources they behave more like second- or even first-order systems, in that they only react after security incidents or legal actions against them.

Even if they manage to control their internal IT security they might not have sufficient "sensors" to detect outside changes in the data protection requirements, such as new laws and their effects. Even worse, they might not be aware of the layers described before (7.2) and therefore don't even have a control system at all for various types of data.

The solution for this is to clearly define business processes on a meta level for all areas, especially IT, so that in fact a third-order feedback system can be achieved:

- Who is responsible for the topic?
  - Does the person have the necessary authority to change the current behavior?

- How can the current state be examined?
  - Types of key data and how to collect them
  - Are we effective?
- Which (internal and external) sensors can be utilized?
  - Monitor the business environment
  - Monitor the legal environment
  - Monitor the social environment
- How will this knowledge be stored and accessed?
  - Keeping it just in the heads of employees creates dependencies and is risky
  - Can we recover from losses or disasters?
- Recombine the knowledge and improve the situation
  - Are the current processes effective?
  - Evaluate the usefulness of the sensors
  - Extrapolate the future environment and invent

7.3.3 Relevance

The first and foremost question for a SMB is of course how and why they should finance (in terms of money and resources) such kind of management and control, since it is perceived as not being relevant for economic survival.

By just looking at IT and data security we can see that the latter assumption does not hold true anymore. The public becomes more and more aware that we are living in an information society and that their data is as valuable as any other of their physical property. This leads to a demand for more legal protection, and especially enforcement of such. Furthermore the public starts to punish corporate misconduct themselves by changing their economic behavior, such as buying from the competition. In the near future it will be therefore mandatory for economic survival to comply with the expected data protection level.

Such a level can only be achieved if a company has control over its processes, in this case over their data handling and the lower layers that support it, the IT department. As described before (7.3.2) this requires business processes, and also meta processes which define a third-order feedback system. Only such a system will be able to adopt in a timely manner to the ever changing IT and legal environment, and also in an effective and efficient way.

7.4 Internal IT

7.4.1 Definitions

A modern, state-of-the-art IT department is the result of a long evolution, in fact such departments already existed before computers were invented. Their duty was to store and manage the business data for the company, at first on paper and starting with the first mainframes also in electronic form.

But the invention of computers allowed and required those back offices to shift from data management to information processing, and this implicated also a shift from passive storage actions to active process design. This shift occurred alongside the DIKW hierarchy:

Data usually known as a collection of symbols, such as the alphabet or numbers

Information on this level some kind of sense has been added, as the collection of data describes something, for example "180cm", "70%" or "25 years"

Knowledge this describes a deeper sense by utilizing predefined information, like "Bob has a height of 180cm, is 25 years old and has an income of 70% in relation to the national median", this is also often described as "how-to"

Wisdom is the ability to understand the structure behind knowledge and therefore shape the existing knowledge as needed, this can be described as "know-why", for example "Bob only earns 70% because in this society younger people are payed less than older ones"

This is a very basic definition of the DIKW model, a more detailed description has been done by Ch. Zins [173].

While most people think of IT in a sense of data or information processor, it is today in fact a knowledge manager and also a tool for wisdom management. On the lowest, technical level the IT department does indeed store information, like emails or text documents. But since it provides also the tools and resulting from this the processes for accessing this information, it manages also the knowledge of the company. And resulting from this it is also the interface and tool to apply wisdom, usually in the form of optimizing processes or through data mining.

The term "information technology department" itself can be considered outdated today, rather "knowledge -" or "process management department" should be used.

In this thesis the term "DIKW" will be used to describe the above mentioned categories in general, and "pDIKW" if their content is related to a person.

7.4.1.1 Conflicts

A definition problem occurs now since the EU legislation always mentions “data” and its protection, but according to the commonly accepted definition above it should rather be “knowledge”. Any personal data consists not only of information, such as “180cm” but is also related to a person, which connects additional meaning to the information and it therefore becomes knowledge.

The legal term should for this reason rather have been “knowledge protection”, and also in in the Austrian case “information” instead of “indirect personal related data”.

In the remaining part of the thesis the scientifically correct terms will be applied, unless a specific law is quoted.

7.4.2 Organizational basics

The IT department itself is not a monolithic block, but rather consists of further sub units. Depending on the size of the company are those units not necessarily implemented as real, independent entities. In an SMB they might even be done by one physical person, who furthermore might even be a subcontractor.

The units can be vertically distinguished by their abstraction level according to the DIKW model, and horizontal by the level of integration with other parties. Each of those combinations is affected in a different way by personal data and security related issues.

	core	back office	end user	external
knowledge flow				
business processes				
applications				
authorization and authentification				
operating system				
hardware				

Table 7.1 IT department units

core The IT environment itself, such as the LAN, servers and storage media

back-office Infrastructure services for the company itself, such as HR and accounting

end-user Internal business users, who utilize the two before mentioned areas to provide services to customers, such as sales, development or customer services

external	Business partners, suppliers and customers, or in general parties outside this legal entity

The top level here is the knowledge flow. It describes who will have access to the business knowledge and in which way. This is the level at which any data protection mechanism has to be implemented first. The design has then to be made top-down, and each following level has to be designed to the needs of the level above, including tools, software and hardware.

Each layer of this model needs to have security considered in its design, it is not possible to add security afterwards or by using some kind of module.

> Security is a process, not a product [166]

If the security of one layer breaks, then all layers on top of it are affected. For example, if the authentification process in an application is broken, then the access rights don't work anymore because it will be possible to assume another, higher privileged identity.

This approach is quite the opposite of how (small scale) IT systems are usually planned: it starts with off-the-shelf hardware, adding the operating system that comes pre-installed and then some commonly used business software is added. Afterwards it is expected to put some business processes on top of that and "security" is added. Obviously this can not work, as every step taken from the bottom upwards limits the possibilities of the next level.

The top-down approach is of course easy to implement if no infrastructure exists yet. Unfortunately in real life there is usually a grown infrastructure that needs to be considered. SMBs do have an advantage here, as they are able to migrate whole levels or systems at once because of the small size of the IT infrastructure and flexibility of the IT department.

For larger corporations this causes a serious problem. Usually they try to solve this by migrating their applications one by one into a new middleware (such as SAP [165]) and then modify the top three layers in there. But this basically locks them in with one vendor and therefore again removes flexibility.

7.4.2.1 ITIL small scale implementation

As described before, it is mandatory to design the IT environment by splitting it up into well defined areas. This idea is not new, and one of the most well known methodologies is the Information Technology Infrastructure Library or ITIL [161].

The full ITIL model is usually not suitable for a SMB, as it would imply too much overhead. Therefore the ITIL small scale implementation [162] was created, which better suits small IT teams.

The core idea of ITIL is to create IT services and provide a framework for their design and operation. This enables a sound control of what is happening

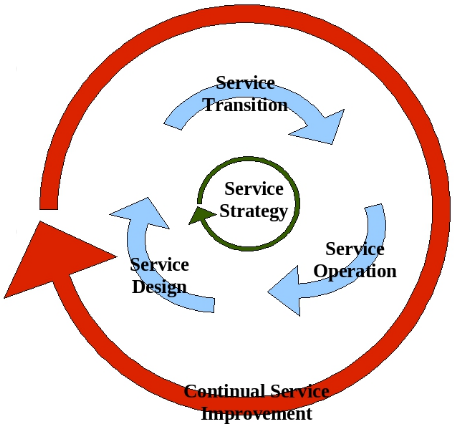

Fig. 7.5 The ITIL service lifecycle

in the IT environment and also enables the IT department to charge the business according to their usage of specific resources. Furthermore it allows monitoring and controlling of the IT services and therefore allows to exercise control over the DIKW usage.

7.4.2.2 Recommended staffing

It can be assumed that a SMB only has limited resources to spend on the IT department. Labor costs will therefore be, proportionally, a rather big part of the while IT costs and therefore should be spent where the most benefit can be gained.

As shown before, the way how and which data is handled has the most influence on the required infrastructure. The staffing question should therefore be approached from a top down perspective, according to the table presented before (7.1). The following numbers of dedicated IT personal are possible:

Zero In this case an external party has to provide the full service, which also means that this party will have a considerable influence on the business processes. Usually this situation should be avoided.

Half Here the IT person will also cover other business areas. A useful combination can be made with managing the back office, since those two areas interact often in regard to data handling and also similar skills are needed for both. It should be avoided to combine IT with business users, such as sales or marketing since this will lead to conflicts of interest, and also the required skill set differs.

One If there is one person dedicated to IT tasks, then his skill set should rather be with information, knowledge and business processes than with technical details. As stated before, DIKW handling needs to be approached top down, and the technical implementation of the lower levels can easily be outsourced if there are not enough resources internally.

Two+ As soon as there is a real IT department, consisting of two or more people, more if not all vertical levels (7.1) can be covered internally. Starting with two people the responsibilities should be split up along those levels, into design and technical implementation, and then refined further when more manpower becomes available.

Depending on the amount of human resources available, the top right part of the table (7.1) should be the starting point, expanding to the left side, and then covering more and more rows downwards as resources are added. This allows the company to focus their in-house resources on those areas where the most relevant DIKW occurs, and avoids dependencies on external parties for business critical processes.

In case of Sweden should the company nominate a data protection officer in any case, even if there is no dedicated IT person. The possibility to handle the registration of applications and other tasks internally bears a very high business value that should not be forfeit.

In general allows this approach to have at least one IT person in charge of the pDIKW flow in and out of the company. This is an absolute requirement to be able to have an overview about which pDIKW is processed and where it is located. Which then is the basis to secure and backup the pDIKW or respond to information requests.

7.4.2.3 Subcontractors and outsourcing

There are two ways of how to utilize external resources:

1. let an external party handle a whole service
2. use external manpower or resources to support an internal team

The first option is usually chosen because of cost reasons or because of lacking know-how inside the IT department. Typically low-level services are affected by this, such as hardware support or end user support regarding standard software. No or very little training is required for the external party to be able to work for the business and the external party can be exchanged rather easily.

The second option is mostly used to help the internal team cope with unusual workloads or one-time projects. The internal team can then focus their effort onto tasks which require a sound understanding of the business and use the external resources for otherwise minor tasks or such where only little local know-how is required. But still this adds some new workload to the internal team, as they now have to manage additional resources.

Both possibilities are sometimes also done in a way that actually has a negative effect on the business, when services are given to external parties which require business know-how or affect a whole business process. In this case the external party becomes part of the company, but as a black box system. This introduces a source of problems into the business process which can not easily be handled.

From a data protection viewpoint is the external party in both situations a subcontractor. This means that whenever an external party is allowed access to pDIKW, a data protection contract has to be signed. If they break the law it will still be the outsourcing company that will be held responsible [3, art. 17]. Although it has been shown that a court, especially in Austria, usually states very low fines for such cases, the cost to the business will be much higher. Customers might lose their trust in the company and business partners might demand cost intensive improvements or audits. Therefore it is important to include a contractual penalty appropriate to the potential business impact, to encourage the external party to implement useful security measures.

In Sweden the outsourcing company actually is required to monitor the operations of the sub contractor [100, § 31], which is in general the approach that should be taken in other countries as well [3, art .17 lit. 2]. As described before, the interest has to be to prevent pDIKW issues and therefore businesses losses, and not only to be legally on the safe side.

If feasible, the external party should work with provided equipment instead of their own, to mitigate at least on a technical level the risk of security holes. This will also allow for easier monitoring of the data protection measurements, as legally required.

7.4.3 Security basics

The DSG and PuL, as well as the EU regulations in general [3, art. 17 lit. 1], require personal information to be protected

- against access by unauthorized parties
- against intended destruction
- against accidental destruction

and furthermore to log any

- access
- modification
- transfer

of it.

This can be achieved by providing the general security services of

- confidentiality

- integrity
- availability

combined with user management for

- authentification
- authorization.

Since pDIKW is handled on all layers of the IT environment (7.1), it also has to be protected on all of them.

While security on the lower layers is rather well understood and deployed today, the top layer, which includes social interaction, is still a big security risk. Malicious hackers, such as the infamous Kevin Mitnick, often gained access to confidential information by convincing employees to ignore company rules. Every employee should therefore on a regular basis be reminded of the security policies, in accordance to the legal requirements such as the DSG and PuL.

Both laws also require state of the art protection in relation to technical possibilities . Here the field of research has to be closely monitored, since measurements that were considered secure in the past could be broken at any time, which would invalidate their usage. Examples are the now obsolete WEP encryption for wireless networks, or passwords and hashes with less than 7 characters, which can be broken today in seconds through freely available rainbow tables [164].

Again it is in the interest of the company to actually train their employees and monitor their compliance, not only for legal reasons but to avoid business losses.

7.4.4 Information and data security

7.4.4.1 Information as a value

First and foremost it needs to be understood that DIKW is a property with value, similar to a physical object. In case of pDIKW the processor is not even the sole owner of it, but rather a trustee, since the affected person itself still holds rights to it and has several titles against the processor.

The processor therefore needs to define the value of the DIKW, based on

- the cost for replacement
- in case of loss, the risk for the person
- in case of loss, the penalty for himself

Based on this value, the required security measurements will have to be planned.

7.4.4.2 Information lifecycle

Like any common good has pDIKW a well defined lifecycle, it is created, used and destroyed.

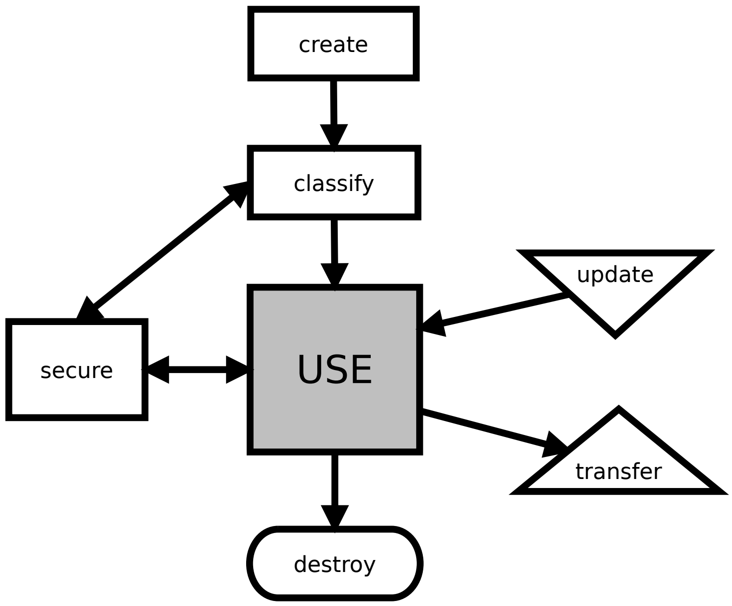

Fig. 7.6 pDIKW lifecycle

Create The pDIKW is gathered from specific sources. This enables the processor to ensure a certain quality, and also to answer the question of origin if a person inquiries.

Classify Here the sensitivity of the pDIKW is specified. Based on it the further handling will be determined. It is economically not feasible to handle all pDIKW at the same level, but legally required for some to be especially protected.

Use Based on the classification, only certain employees should have access to the pDIKW (“need to know” principle). Furthermore the law mandates that any usage has to be logged.

Transfer As soon as a subcontractor is used, a similar cycle has to be defined within his organization. It is the responsibility of the processor to monitor this.

Update It is mandated that any personal information has to be current, depending on its usage.

Secure As described before can security measurements become obsolete during the lifetime of the pDIKW. The legal requirements are that security has to be provided according to current technical possibilities, therefore a periodical evaluation is required.

Destruction When the underlying purpose of the pDIKW ceases to exist, it needs to be destroyed. Failure to do so leads to unsecured and outdated pDIKW, which has no business value but can lead to liabilities.

Especially the last step, destruction, is usually an unaccustomed concept for companies. Falling prices for storage media and advancing methods for data mining give the impression that more pDIKW equals more value. It is often forgotten that pDIKW needs to be secured and updated, which is a costly process. Furthermore it can be argued what business relevance might be left after several years.

7.4.5 Physical security

At the lowest level, the physical entities which hold pDIKW need to be secured.

This starts with mandatory access controls to the rooms and buildings where pDIKW is processed, which is even explicitly required by law. Common mechanisms are a mandatory check-in at the reception and key cards or similar controls for server rooms.

Any end users device need to have a log in system, so that any usage can be attributed to a specific person [3, art. 17 lit. 1]. This includes not only common PCs, but also laptops, smart phones or any other device that provides access to pDIKW.

If there might be situations where pDIKW is stored or cached locally on a device, then further protection is needed, or otherwise an unauthorized person might gain access to it in case of loss, theft or reuse. Since the actual data medium, such as a hard disk, can more or less easily be retrieved from a device, thereby bypassing any security mechanism that might exist in software, the only way to accomplish protection is through full encryption of the medium. Thus only the authorized user will be able to work with it. The most common tool for PC platforms is the Open Source software TrueCrypt [169], but there are also commercial solutions which can be integrated into an enterprise wide authentification system.

7.4.5.1 Physical media lifecycle

Users often transfer pDIKW to other users by transport media, such as USB sticks, therefore those have to be included in the protection concept.

Since such an extension results in the end in more costs, it first has to be determined if such a transfer is necessary at all. End users often utilize such media because the existing system makes other ways of transfers unfeasible, for example by providing bad usability, low speed or by not providing such a service at all. The highest priority should therefore be given to solve the issue already at this level. Another issue arises from the fact that by using a transfer medium existing authorization and authentification systems are usually circumvented, which might already be against the law [3, art. 17 lit. 1].

If a medium is required, then it needs to be at least encrypted. That way a certain level of authorization can be implemented, and also protection against theft (of the pDIKW) is given. In the case of USB sticks can this be conveniently realized by distributing them centrally and pre-installing encryption software on them.

When unencrypted media are used more precaution needs to be taken. Every medium should be identifiable, such as by a printed serial number. Possession of it should be registered and confined to secured areas. The latter can be realized through RFID tags which set off an alarm when a certain area is left.

During their lifetime media need to be tested for integrity. Items like CDs or DVDs deteriorate over time, and after a while the legal requirement of protection against accidental loss [3, art. 17 lit. 1] is not fulfilled anymore. Such media should therefore also not be used as the only occurrence of certain pDIKW sets.

When the medium or the pDIKW on it reaches its end of life, the medium needs to be securely overwritten or destroyed, depending on the storage technology. While it has been shown for hard disks [171] that common "secure deletion" programs, such as DBAN [154], really do remove any data beyond recoverability, the same might not hold true for other technologies. In such a case the medium has to be physically destroyed. Examples are USB sticks, backup tapes, CDs, DVDs or Flash memory cards.

It should not be forgotten that log files often contain pDIKW as well, and therefore their physical medium has to be treated in the same way.

7.4.6 Design of applications and services

Modern application or services are usually designed in multiple layers, such as the user interface, the business logic and the database access. The issue of pDIKW has to included from the beginning in this design, or otherwise personal and non-personal DIKW might be mixed together unnecessarily. This would extend the area which needs special protection and thereby inflicts avoidable costs.

Again a top down approach should be taken. The combination of personal and non-personal DIKW should happen as late as possible, which allows to have two distinguished technical areas. This separation should then continue down to the lowest technical layers. Examples could be

- separate file servers for pDIKW and marketing material
- separate databases and servers for the inventory and sales system
- specific printers and printer queues on different servers for marketing material and customer communication
- different websites and infrastructure for providing technical information and the online web shop

Apart from technical diagrams about the infrastructure, the IT documentation also has to include a flow diagram for pDIKW. Only that way can systems with special protection needs be identified and their access logged in an appropriate way.

If such a separation is not possible because the IT infrastructure is so small, then the whole environment must be secured adequately to the the most sensitive pDIKW found on it. Up to a certain size this will actually be economically more feasible than managing the pDIKW flow at all.

7.4.6.1 Backup and storage

To protect against accidental loss, one part of the IT requirements is to have backups of all DIKW. Usually an economic decision about the need for backups is made based on the costs to recreate the lost DIKW. This is not valid in case of personal related DIKW, since the law requires to protect against accidental or deliberate loss in any case [3, art. 17 lit. 1]. Backups are therefore mandatory.

The "need to know" principle can be applied here in the way that the person who is handling the backup should not have access to the actual pDIKW on it. Thus the requirement for any further protection measurements can be avoided. This can be done by creating the backup set inside the system and then only writing out an encrypted block to the backup medium.

An example would be a database backup script which exports the daily changes, encrypts them and then writes this record to a tape drive. That way the handling of the tapes could be done by regular staff, such as a secretary in a remote branch, without coming in conflict with data protection laws. It also mitigates risks in case of theft of the medium.

7.4.6.2 Using external services

Nearly no company works independently nowadays, the usage of third parties for specialized services is rather common. Usually the processor is aware that he is giving pDIKW to another party and therefore has to apply the legal requirements, such as in the case of using a credit score provider. In other cases this might not be so obvious, for example:

- Hiring a specialist as a subcontractor, instead of as an employee, to work on specific pDIKW set
- Using a web statistics provider, such as Google Analytics [158], who evaluates the customers IP addresses and their behavior on the web page
- Using a CRM system that is hosted by a third party for managing and sending marketing emails
- Using HTML code in emails to track their reading through a third party service provider

In all of those cases pDIKW is processed by a third party, which requires a service contract, monitoring by the processor and so forth [3, art. 17].

It has therefore to be considered during the design phase of an application, what parts are economically and legally feasible to be outsourced, and which are too risky from a security and liability perspective.

7.4.7 User and identity management

One central legal requirement is authentification, authorization and logging [3, art. 17 lit. 1]. Only those users who have been instructed to work on specific pDIKW should have access to it, and any usage has to be logged. This covers not only the actual applications, but also access to files or physical access - in the end all layers of the IT infrastructure (7.1) need to be covered.

Most operating systems already provide tools to monitor file access, but not all off the shelf applications do so, which means that they can not be used for pDIKW.

A user identity also has a lifecycle, similar to the DIKW one, with the additional effect that this becomes pDIKW itself, since it is related to a person (the user). This recursion has to be taken into consideration when designing the IT environment. As soon as biometric DIKW is involved it even becomes sensitive data in the terms of the law [3, art. 8 lit. 1].

Also the requirement of non-excessive data usage needs to be observed [3, art. 6c]. It depends on the sensitivity of the pDIKW which kind of identification properties can be used, such as name, photograph, fingerprints or other biometric systems.

7.4.7.1 HR interface

The first and last step within the lifecycle of an user identity will be done through the human resources department.

When a new employee joins the company the following steps are required:

- general information about the data protection laws, especially his obligation to secrecy even after the end of his employment
- instructions about the approved usage of the IT and back office environment
- instructions about pDIKW usage [3, art. 16]
- optional in Sweden: information about the “personuppgiftsombud” and his role
- optional in Austria: information about existing “Betriebsvereinbarungen” with the workers’ council

This information should be handed out in written and confirmed through his signature.

Although there are no explicit legal requirements given when an employee leaves the company, the following steps should be taken:

- signed confirmation that he does not hold any company devices or media anymore
- signed confirmation that he did not leave any of his private DIKW on company devices or media
- suspension of all his software accounts and access tokens

For technical reasons it is often not possible to simply delete user accounts, since this might interfere with the integrity of log files or other databases. Instead the account should be disabled, or if not possible, protected with a maximum length random password.

The HR department will most definitely be handling sensitive data in terms of the law, since they need to process medical information, such as the duration and reason for a sick leave, or results from job assessments. For this reason, and also because of the general higher sensitivity of their pDIKW, should their IT infrastructure be separated from other departments. Otherwise they might contaminate, in a legal sense, for example a regular file server, and then the whole server would have to be protected on this high level.

7.4.8 Monitoring and surveillance

All affected employees or third parties have to be made aware of the monitoring. In case of cameras it needs to be done through signs, and in case of software it should be included in the signed working contract. Furthermore should this information readily be available to all employees.

There are four general situations where monitoring of employees or other parties can occur. In all of those cases has this to be considered processing of pDIKW which leads to legal requirements.

7.4.8.1 Required by the law, such as logging usage of pDIKW

This has to be included into the application design as described before, but also mechanisms of the operating system might be needed if the pDIKW is accessed on a plain file level. While common text files, such as a letter, are unstructured data, the same can not be assumed for a spread sheet. According to the law [3, art. 2 lit. c], if it can be accessed by multiple criteria then it is considered a data application. This holds true for any list in a spreadsheet, since it can easily be sorted or searched by each column. It might therefore require a registration, but definitely needs to be monitored for any access.

7.4.8.2 Desired by the company to protect their property

The usual approach is to use video cameras, which requires the consent of the employees. As discussed before, the legal requirements are rather easy to handle in Sweden. Austria further distinguishes among technical details, which is why there an old fashioned analog surveillance system with limited recording should be preferred.

7.4.8.3 For technical reasons to manage utilization and provide technical protection

Often the IT operators log a lot of application or access data, because it is easy to enable and a common setup. Unfortunately this includes usually pDIKW and they might not be aware of the legal consequences. Examples would be the logging of access to filtered websites, login and logout times or email server logs.

It should be analyzed which logs really bring a tangible benefit at all, and where also the identification of the user is required. If there is no justified cause, then pDIKW can not be processed. Especially for utilization statistics can it be sufficient to rather log anonymized data.

Replacing the actual identifier, for example an IP address, with a hash value is only possible for external cases. In internal cases it can be argued that, for example by hashing all internal IP addresses, the original identifier can always be looked up again.

7.4.8.4 Digital forensics

If there is evidence that a criminal act has been committed by using a computer on similar device, then it needs to be secured and investigated for further legal actions. Although this most probably will include pDIKW, such usage is covered by the exception for criminal proceedings [3, art. 13 lit. 1].

But since usually an external specialist will commit this analysis, a contract has to be made with him and all other legal requirements for subcontractors need be observed since the exception only applies to the processor himself.

7.5 Business to customer

7.5.1 Homepage

There should be a separation between the rather static informational homepage and dynamic content such as web shops and forums. Both parts have different security requirements and also a different userbase that may want to make changes. At least a different subdomain should be used, such as "webshop.company.com", and if possible it should be placed on a different server.

The static page can be outsourced to a hosting provider, since it will not contain pDIKW, also it will receive the most traffic which would otherwise add costs to the local Internet bandwidth requirements.

The dynamic content on the other hand will only be visited by customers who consider to buy goods or want to participate in discussions, and therefore needs to be integrated with internal IT systems. This leads to higher security requirements which can be best fulfilled if everything is within one system and location. If this can not be done, then the provider hosting the dynamic content is considered a subcontractor and the processor has supervising obligations.

Both sites need to be secured through the HTTPS protocol, the web shop for apparent security reasons. But even the static page may be altered during transfer by some providers who experiment with adding advertisements to HTML code they transfer [163]. Since this is not apparent for the customer, he will accredit the whole content to the company which then could lead to legal consequences.

To further secure the static site, a content management system (CMS) can be used internally to build the site, but then will be exported as plain HTML code. That way no dynamic functionality, which is prone to attacks, is exposed to the Internet. This externally visible content can also be regularly compared to the internal version by a monitoring script to detect successful hacks ("defacement") in a timely manner.

External graphics, such as advertisements or product pictures from a supplier, should never be included indirectly (embedded), since they might be exchanged with malicious content at the third party's site. They would also allow the external party to monitor which clients are accessing the site, which is a leak of pDIKW and can be hold against the company. Instead a local copy needs to be used, which can also be converted to another image format to render malicious data streams ineffective.

When using external services on purpose it has to be investigated if pDIKW will be involved. In such a case the external party is a subcontractor and all legal obligations apply [3, art. 17 lit. 2]. This is often overlooked when using services such as Google Analytics [158] or other tracking services. They utilize the customer's IP and other pDIKW, and are often even located outside the EU, which constitutes therefore a transfer to a third country. This might even already be the case when pictures or other data are embedded from a third party.

7.5.1.1 Static content

If internal information about the company should be published, then the consent of the employees is needed when publishing information about them. Common examples are pictures of employees or of company meetings. While the publishing of contact information, such as name, phone number and position is allowed, further information might be problematic. Especially medical information ("is currently sick") has to be avoided at all [3, art. 8 lit. 1]. The work contract with each employee should clearly state what pDIKW about them will be made publicly available.

An imprint needs to be available, in Sweden easily accessible and in Austria further more accessible from every page.

7.5.1.2 Dynamic content

A lot of current CMS or web shop products have severe security issues, such as being prone to SQL injection. Since the law requires up to date protection measurements, those systems need to be monitored and updated as soon as a patch is available. This might be more easy for a dedicated provider, who serves a multitude of customers, than for a small company, which has to be taken into account when deciding about local or remote hosting.

There is no obligation for the processor to monitor user content proactively, but he needs to act as soon as he becomes aware of unlawful content [8, § 14]. While this does not result in a requirement for 24x7 monitoring, for a regular business, it still can be a problem if the responsible IT person is on vacation or otherwise unavailable. If a SMB wants to accept user content then they need therefore to provide the necessary human resources.

In case of Sweden it should be checked if an "utgivningsbevis" can be applied for, as this would add further protection.

7.5.1.3 Web shop

In addition to the consideration for dynamic content the requirements for electronic commerce need to be observed, such as the extended imprint in Austria.

When receiving customer orders through the web shop, no automatic order confirmation should be generated through it. Since the web shop might have a security weakness, a fraudulent order may be generated which would be hard to legally challenge if it was already confirmed through the site. Instead each order needs to be approved by an employee.

Also the order process has to be separated from the technical communication. The fact that an email was received or confirmed by an email server does not constitute the acceptance of an order. Such events need to be stated explicitly.

7.5.2 Marketing

7.5.2.1 Data collection

For private customers the usage of their pDIKW is always an opt-in situation, therefore when using it for marketing it can only come from three sources:

- Existing pDIKW about current customers; this can only be used for advertising in the same business area where his pDIKW originated from
- Gathering new pDIKW from customers; in this case they have to agree to the usage
- Buying pDIKW from commercial database providers; here the provider or seller has to prove that the people in their database have agreed to the usage

If the company collects the data themselves, then apart from informing the customers about it, they should also explain where the value for the customer is in it. Otherwise the collected data will be incomplete or wrong. Especially in situations where a company tries to force customers to divulge pDIKW because they otherwise won't have access to information, such as software updates, the customer will often simply provide false data which is then of no use to the company but still inflicts costs for protection.

7.5.2.2 Advertising

Any form of personalized advertising needs to provide an opt-out mechanism, such as a HTTP link in an email. This has to remove the customer permanently from further campaigns; sending a reminder for example one month later to ask if he was sure or wants to join again is not valid.

As with web sites, when using third parties for advertising they have to be considered subcontractors with all legal consequences [3, art. 17 lit. 2]. It should therefore be avoided to use common Internet messaging or CRM services, which may be hosted outside the EU, for personalized campaigns. Apart from this issue will the advertisement often be filtered by the customer since it originates from well known "spam" sources.

7.5.2.3 Social media accounts

With the advent of "Web 2.0" services more and more companies try to communicate with their customers through sites such as Xing [172] or Facebook [157].

This is a gray legal area without any court decisions yet. It can be argued that the customer publishes his pDIKW by his own free will and then informs the company about the location. In this case the pDIKW won't be protected. Another argumentation would be that the company uses the web service as a subcontractor to enable people to share their pDIKW with them, in which case the data protection laws fully apply [3, art. 17 lit. 2]. As a general rule, when contact information is managed through such a service, then it has to be made sure that the customer contacts the company first as this can be considered an opt-in act.

A second problem area is that of account ownership. It needs to be clearly stated internally that only company-provided service accounts may be used to conduct business. The IT department needs to provide a mechanism so that the company can always reclaim ownership of the account in case an employee changes the password or otherwise tries to make it unavailable to the company. A similar problem exists if an employee uses his own private account for business purposes, for example when a sales person manages his customer contacts that way. Apart from the legal issues with pDIKW in that case, the business information is lost when this employee leaves the company. No law case has so far been done in Austria or Sweden to investigate this area.

7.5.3 Job applications

In case of a SMB should job applications only be handled through email or paper. Building an applicant database, such as often seen in large corporations, has very limited value for a SMB but instead leads to higher security requirements and therefore higher costs.

Since pDIKW may only be processed for a specific purpose and the time needed [3, art. 6 lit. 1], the HR department needs to collect those emails in a separate mail folder, which allows for easy destruction once the new employee has been determined. If there are paper printouts or letters then they need to be handled in the same way.

If the applicant sent code examples or other copyright protected material then it has to be made sure that all copies are destroyed afterwards. Otherwise he might claim later on that the company used his ideas for their own purpose which could lead to intellectual property liabilities.

7.6 Business to business

The same tools as in the B2C case can also be used for B2B, but usually there is an opportunity for further automated integration. In the case of a SMB however it has to be evaluated if the long term cost reductions and efficiency gains justify the high entrance costs into this technology. Systems of automated order processing and contract signing through certificates need up front investments into hardware and knowledge, which means costly man power. It can be argued that the smaller the company, the less economically feasible will such a solution be. With the same reasoning the situation at the other company needs to be considered. The technology can not be utilized if the partner is not at the same technical level, or can not provide sufficient IT security.

In general the same protection requirements as in the B2C area are given, with the exception that Austria gives pDIKW about companies the same level of protection as that of private persons, while Sweden differs between those. In practice this does not make such a big difference, since often information about contact persons at the partner company will be handled, which then constitutes pDIKW even in Sweden. Therefore should no further distinction be made in practice between B2C and B2B pDIKW when designing the security requirements.

7.6.1 Unstructured data handling

At very small companies no real business database might exist, instead most of the work is done manually and even accounting is handled by an external specialist. But there are still common situations where the full data protection laws apply:

- Although the work is done on paper or text documents, which can be considered unstructured collections, contact listings are often handled through spreadsheets or address lists in the email client. Both of those are struc-

tured databases, as described before, and are therefore considered data applications.
- If the tax consultant compiles a list of the companies business partners to simplify his work, then he is also utilizing a data application. In this case he is doing it by instructions of the company, or it may be argued that he does it illegally if he has not been instructed so. In the first case the company is still in the role of a processor who utilizes a subcontractor, and therefore is fully responsible for the protection of the DIKW [3, art. 17 lit. 2].

7.6.2 Signatures

If electronic transactions will be done between two parties, then they need to be signed by electronic signatures to provide the necessary protection. The legal basis for this has been done through an EU directive [7] which has been adopted into national law, but according to an EU survey [155] the resulting implementations differ across the EU. In regard to Austria and Sweden the study highlights the following points:

- Although there are no legal obstacles to use certificates between the two countries, interoperability issues and regulations have led to isolated "island" solutions where cross border applications are rather difficult.
- It is rather difficult and expensive for the providers of the necessary hardware to get it certified. Only in Austria are more than two devices available.

It can be said that it is in general more easy to utilize signatures within a country than across borders. Still Austria is in general below the EU average when it comes to B2B usage and even Sweden has room for improvement [156].

As a side note, even if two business partners do not want or can not use (qualified) certificates based on the EU directive, they still can use other or self signed certificates combined with a frame contract. But this will not be covered by the local signature legislation since it is just a regular business agreement.

There are differences in which cases a signature can be applied. In Austria it is considered equal to a handwritten signature, while it is in Sweden rather another method of signing that needs to be agreed on or have a legal base. It is therefore necessary in Sweden to include an agreement into the terms and conditions or a frame contract.

7.6.2.1 Signature lifecycle

First, as discussed before, it needs to be evaluated if the costs for handling the signature are worth the benefit.

Technical and organizational procedures need to be in place in case the signature is lost or stolen. A backup of it will need additional protection, such as encryption, to avoid misuse or duplication of the backup version. If the certificate is attributed to a person, it even becomes pDIKW and therefore requires further protection.

Apart from becoming unavailable, the signature will also have to be updated or replaced after it becomes invalid. This can happen because its validity expires or when technical progress makes the cryptographic algorithms in use obsolete. Processes are required to make sure that already signed data can still be used, or re-signed with the new one.

Also the access to the signature needs to be managed. Austria only allows certificates for physical persons, therefore every affected employee will require his own one. While Sweden also allows a certificate for a company, it should internally be further protected again by individual certificates who then allow access to the company certificate.

7.6.2.2 Invoices

A common use of signatures will be for electronic invoices. Current law requires qualified signatures for this, but as mentioned before a new EU directive [27] amends this.

SMBs should therefore wait until this amendment is implemented into national law, and then agree with their business partners upon a simplified version of security, such as self signed certificates that are only used between those two parties, or encrypted PDFs together with a weekly summary as a protective measurement.

7.6.3 Automated transactions

By utilizing digital signatures business partners can implement automated transactions in a legally sound way. Examples can be automated orders, originating from project data out of the ERP systems or executed by falling below a certain inventory stock.

It has to be taken care that such actions do not affect physical persons, since otherwise the legislation about automated individual decisions [3, art. 15] will be applicable.

Otherwise no explicit legal requirements are given, but common IT and process security measurements should be employed:

- Using an encrypted VPN communication tunnel
- Doing sanity checks on outgoing and incoming transactions and rejecting suspicious ones - this needs to be covered by the frame contract
- Exchanging summary information on a regular base, which is then checked by a human

7.7 Conclusion and recommendations

A company that aims to follow the EU regulations in regard to data protection can orientate itself by the examples of Austria and Sweden.

7.7.1 Technical and organizational

The primary task is to create an IT environment that is actually able to follow and focus on the flow of DIKW. While this is not only an advantage for handling the legal issues, it also aids the company in defining the best business processes for its value chain.

Based on this the actual architecture and design of the IT should be done. This allows then for an easier identification of pDIKW, and the application of the legal requirements for it.

A European company needs therefore to understand that it handles virtual goods (pDIKW) in the first place, and then, as a result of this, physical goods.

While the current IT education aims to support such an environment, the awareness in other business areas will be insufficient. The more difficult task for a company will be to train its non-IT staff to handle pDIKW with the proper care. The idea that pDIKW is a valuable good that needs to be protected and processed according to set rules is unfortunately not part of the common educational system.

7.7.2 Legal

Although Austria and Sweden are similar, they differ in their implementation of the EU legislation. The same can be expected from the other member states, which therefore requires a company to research all individual details.

But by comparing the EU legislation with the examples in Austria in Sweden it can be shown that the deviations are not too severe. Generally the business philosophy should include these points:

- Inform the client when pDIKW is collected and for what reason
- Secure and monitor access to the pDIKW

  - Ensure the same during outsourcing
  - Restrictions exist for business partners outside the EU

- No hidden surveillance or log evaluation
- Be identifiable to all customers
- Use qualified signatures for electronic commerce

The area of electronic DIKW processing is rather new, from a legal perspective. The laws and regulations are therefore still in motion, and the situation changes every year, as for example with the electronic invoices [27, art. 233]. It is therefore mandatory for a company to monitor the legislation process on the EU and national level, and also observe local court decisions in their countries of operation.

Chapter 8
Conclusion

8.1 General

Apart from the geographic size, Austria and Sweden seem to be similar countries. Both have about the same population, similar population distribution over some major cities and otherwise rural land, and also a comparable political history. Even their economic history during the last 50 years has similarities, growing from a rather agricultural society into a modern one with a mixture of industry, service and information areas.

But when looking at the society, and the expectations that the citizens have about their government, significant differences can be observed. Those led in the end to different practical realities in how data protection is handled in those two countries.

If a company plans to conduct business in Austria and Sweden, then the legal requirements in regard to data protection will be not too different. Although Sweden offers some advantages through an internal data protection officer, the basic requirements about how personal data has to be handled are similar. Austria tries to simplify some issues by allowing the local workers' council to make agreements instead of their members, but this catches only the data handling between the employer and the employees.

Also the obligations for providing services over the Internet are comparable, only the handling of video surveillance differs noticeable.

The actual differences arise from how the company will be treated by the public and by their business partners. The fact that here is little pressure from the government in Austria and the rather bureaucratic handling of the registration has led to a climate in which the protection of personal data does not have a very high priority, unless it can lead to direct business losses. In Sweden, on the other hand, the public demands protection by their government, and is also very sensible to breaches by a company. Trust is in general highly valued. This has led to a climate where companies see data protection as a real business value.

It can therefore be concluded that a company needs to implement similar technical solutions in both countries, but different business processes have to be employed. While the reaction in Austria has to focus on the legal aspects, in Sweden the potential loss of trust has to be mitigated.

8.2 Limitations

This thesis focused on the issues of protecting personal data and conducting business on the Internet. While those areas have been covered in detail, adjacent legal topics have only been given an introduction. Issues such as copyright, contract law or liabilities can be named as examples. Such topics also need to be taken into consideration, but since there is sufficient existing literature available they have been left out here.

Furthermore the provided cheat sheets give an overview and guideline to an interested IT person. But without further education in data protection and practical work with actual issues they will not be sufficient to fully implement a legally watertight data processing environment.

Also the history of how the government is build up and acts in both countries, as well as the political background about how the current legislation came into existence is left out, since this is mostly of historical or sociological interest.

Chapter 9
Appendix

9.1 Cheat sheet Austria

9.1.1 Validity of data collection, processing and transmission

9.1.1.1 Prerequisites [31, § 6]

- For a specific purpose, and
- only in the necessary amount, and
- only for the necessary time

9.1.1.2 Register requirements [31, §§ 16-19]

- None, if
  - only public available data, or
  - only indirect personal related data, or
  - covered by a template application
- May only start after a positive approval by the DSK, if
  - sensitive data, or
  - information about criminal convictions or similar, or
  - information about credit ratings, or
  - part of an interconnected information processing system
- May start together with the application in any other case

9.1.1.3 Processing

- Of personal data[31, §§ 7-8]
  - legally published information, or
  - consent of the person, or
  - to fulfill a contract between the controller and the person
- Of sensitive data [31, §§ 7, 9]
  - published by the person beforehand, or
  - in form of indirect personal related data, or
  - consent of the person, or
  - required to fulfill legal obligations as an employer, or
  - for medical usage if handled by medical personal who are bound by their duty to observe secrecy

9.1.1.4 Cede ("überlassen") [31, §§ 10-11]

- Definition
  - using a third party for processing the data, and
  - the controller stays responsible for any misuse
- Obligations of the controller
  - contract with the third party to ensure that they comply with the DSG, and
  - monitor the fulfillment of this contract, and
  - have a written documentation about the obligations described below
- Obligations of the third party
  - use the data exclusively for the purpose given by the controller, and
  - only use personal that is legally bound to observe the data secrecy, and
  - only use other subcontractors if approved by the controller, and
  - has to destroy the data after the contract ends

9.1.1.5 Transfer ("übermitteln")

- Definition
  - Providing the data to a third party for their own purpose, or using the data internally for another than the stated purpose.
- Requirements

  - The same rules as for processing (9.1.1.3) apply.

9.1.1.6 Cede or transfer to another country [31, §§ 12-13]

- The requirements for cede or transfer as stated above need to be fulfilled in any case.
- No DSK approval is required for
  - European Economic Area, or
  - countries with equivalent protection (5.2.8), or
  - data that is publicly available in Austria, or
  - data that is only indirect personal related for the recipient, or
  - transfers with the consent of the person, or
  - to fulfill a contract between the controller and the person, or
  - data from an application that did not require a DVR registration
- DSK approval is required beforehand
  - in any other case

9.1.2 Data protection requirements for processors

- Protection against loss and accidental or illegal destruction of data
- Protection against access by third parties
- Clear orders to employees about what they may or may not do with the data, and provide them with permanent access to those orders
- Educate the employees about their duties according to the DSG [31, § 15]
- Control physical access
- Control logical access to programs and data
- Log any access to the data
- Document the measurements that are taken to fulfill the above
- Any documentation has to be kept for three years

9.1.3 Imprint

Required on any web page and other business communication, such as emails:

- Company name
- Company register number and responsible court
- Geographic address
- Legal form

This can be simplified by providing a link to the corresponding “Firmen A-Z” WKO page [88].

9.1.3.1 Order forms

In addition to the above stated, web order forms also need to provide

- a copy of the terms and conditions that can be downloaded

9.1.4 Shortcuts

9.1.4.1 Relevant organizations

- DSK: http://www.dsk.gv.at
- DSR: http://www.datenschutzrat.gv.at
- Wirtschaftskammer Österreich: http://firmen.wko.at
- RTR: http://www.rtr.at
- ARGE Daten: http://www.argedaten.at
- RIS: http://www.ris.bka.gv.at

9.1.4.2 Documents

- Registering a data application:
  http://www.dsk.gv.at/site/6296/default.aspx
- Template contracts according to the DSG:
  http://www.dsk.gv.at/site/6208/default.aspx
- Various templates by ARGE Daten:
  http://www2.argedaten.at/php/cms_monitor.php?q=MUSTERBRIEFE

9.2 Cheat sheet Sweden

9.2.1 Validity of data collection, processing and transmission

If the application is covered by the TF [93], such as through an “utgivningsbevis”, then no further rule needs to be applied [100, § 7].

9.2.1.1 Prerequisites [100, § 9]

- For a specific purpose, and
- only in the necessary amount, and
- only for the necessary time

9.2.1.2 Register requirements

- None, if
  - a data protection officer exists [100, § 37], in which case he has to keep a register
- May only start after a positive approval by Datainspektionen, if
  - there is no data protection officer, or
  - genetic information is processed

9.2.1.3 Processing

- Of personal data [100, § 10]
  - consent of the person, or
  - to fulfill a contract between the controller and the person

Data may not be used for direct marketing if the person requests so.

- Of sensitive data [100, §§ 13-19]
  - published by the person beforehand, or
  - consent of the person, or
  - required to fulfill legal obligations as an employer, or
  - for medical usage if handled by medical personal who are bound by their duty to observe secrecy
- Of the Swedish personal number ("personnummer") [100, § 22]
  - consent of the person, based on a really free choice, or
  - reliable identification is required

9.2.1.4 Subcontractor ("personuppgiftsbiträde") [100, §§ 30-31]

- Definition
  - A subcontractor is a third party that processes data on behalf of the controller.

- Obligations of the controller
  - Contract with the subcontractor which allows him only to use the data according to instructions, and requires him to protect the data according to [100, § 31]
  - Investigate beforehand if the the subcontractor is able to fulfill this obligation, and afterwards control that the protection is in place and used
- Obligations of the subcontractor
  - Use the data exclusively for the purpose given by the controller

9.2.1.5 Transfer

- Definition
  - Providing the data to a third party for their own purpose, or using the data internally for another than the stated purpose.
- Requirements
  - The same rules as for processing (9.2.1.3) apply.

9.2.1.6 Cede or transfer to another country

The EU and European Economic Area is not considered a third country.
Otherwise the transmission is allowed in case of

- countries with equivalent protection, as listed in 5.2.8, or
- consent of the person, or
- to fulfill a contract between the controller and the person

9.2.2 Data protection requirements for processors [100, § 31]

- Provide adequate organizational and technical protection of the data, depending on the sensitivity of it

9.2.3 Imprint [105, § 8]

- Name

- Address
- Email address

And, if applicable

- Organizational number
- Tax number
- Regulatory agency

9.2.3.1 Order forms

In addition to the above stated, web order forms also need to provide [105, § 13]

- A copy of the terms and conditions that can be downloaded

9.2.4 Shortcuts

9.2.4.1 Relevant organizations

- Datainspektionen: http://www.datainspektionen.se
- Konsumentverket: http://www.konsumentverket.se
- RTVV: http://www.rtvv.se
- Supreme Court: http://www.hogstadomstolen.se

9.2.4.2 Documents

- Registering a data application or data protection officer: http://www.datainspektionen.se/ladda-ner-och-bestall/informationsmaterial/blanketter/
- Utgivningsbevis: http://www.rtvv.se/se/Internet/utgivningsbevis/

References

1. EU, “1980 Rome Convention on the law applicable to contractual obligations (consolidated version)”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41998A0126(02):EN:HTML
2. EU, “Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:HTML
3. EU, “Directive 95/46/EC of the European Parliament and of 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”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
4. EU, “Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML
5. EU, “Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:EN:HTML
6. EU, “Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0084:EN:HTML
7. EU, “Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML
8. EU, “Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (’Directive on electronic commerce’)”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML
9. EU, “Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:EN:HTML
10. EU, ”Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML

11. EU, "Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML
12. EU, "COMMISSION DECISION of 15 June 2001on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001D0497:20050401:EN:HTML
13. EU, "2002/16/EC: Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0016:EN:HTML
14. EU, "Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML
15. EU, "Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:EN:HTML
16. EU, "Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:HTML
17. EU, "Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML
18. EU, "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)", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
19. EU, "Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065:EN:HTML
20. EU, "Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R0733:EN:HTML
21. EU, "Commission Regulation (EC) No 1496/2002 of 21 August 2002 amending Annex I (the rules of jurisdiction referred to in Article 3(2) and Article 4(2)) and Annex II (the list of competent courts and authorities) to Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R1496:EN:HTML
22. EU, "Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004)", retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R(01):EN:HTML
23. EU, "2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alter-

native set of standard contractual clauses for the transfer of personal data to third countries”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:EN:HTML

24. EU, “Commission Regulation (EC) No 2245/2004 of 27 December 2004 amending Annexes I, II, III and IV to Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2245:EN:HTML
25. EU, ”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“, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:EN:HTML
26. EU, “Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:347:0001:01:EN:HTML
27. EU, “Council Directive 2010/45/EU of 13 July 2010 amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing”, retrieved 2010-10-16; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:189:0001:01:EN:HTML
28. EU, “Study on the implementation and effect in Member States’ laws of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society “, retrieved 2010-10-16; http://ec.europa.eu/internal_market/copyright/studies/studies_en.htm
29. Bundeskanzleramt Österreich, “Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz - ArbVG)”, retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10008329
30. Bundeskanzleramt Österreich, “Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV)”, retrieved 2010-10-16; http://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=20000312
31. Bundeskanzleramt Österreich, “Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)”, retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10001597
32. Bundeskanzleramt Österreich, “Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010)”, retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2009_I_133/ BGBLA_2009_I_133.html
33. Bundeskanzleramt Österreich, “Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister- Verordnung 2002 - DVRV 2002)”, retrieved 2010-10-16; http://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=20001762
34. Bundeskanzleramt Österreich, “Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG)“ retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=20001703
35. Bundeskanzleramt Österreich, “Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen wer-

den (Konsumentenschutzgesetz - KSchG)", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10002462
36. Bundeskanzleramt Österreich, "Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Mediengesetz - MedienG)", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10000719
37. Bundeskanzleramt Österreich, "Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG)", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10005792
38. Bundeskanzleramt Österreich, "Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG)", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10003685
39. Bundeskanzleramt Österreich, "Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 - SigV 2008)", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=20005618
40. Bundeskanzleramt Österreich, "Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004)", retrieved 2010-10-16; http://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=20003495
41. Bundeskanzleramt Österreich, "Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003)", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=20002849
42. Bundeskanzleramt Österreich, "Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen (Unternehmensgesetzbuch - UGB)", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10001702
43. Bundeskanzleramt Österreich, "Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz).", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10001848
44. Bundeskanzleramt Österreich, "Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf elektronischem Weg übermittelte Rechnung bestimmt werden", retrieved 2010-10-16; http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=20003090
45. Österreichische Datenschutzkommission, "Österreichische Datenschutzkommission", retrieved 2010-10-16; http://www.dsk.gv.at
46. Österreichische Datenschutzkommission, "Datenschutzbericht 2007 der österreichischen Datenschutzkommission", retrieved 2010-10-16; http://www.dsk.gv.at/DocView.axd?CobId=30637
47. Österreichische Datenschutzkommission, "Datenschutzbericht 2009 der österreichischen Datenschutzkommission", retrieved 2010-10-16; http://www.dsk.gv.at/DocView.axd?CobId=40344
48. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K600.049-424/0001-DVR/2008/00", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer= DSKTE_20080206_K600.049-424_0001-DVR_2008_00

49. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K120.810/005-DSK/2002", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20020604_K120810_005-DSK_2002_00
50. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K120.657/8-DSK/00", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20000427_120657_8-DSK_00_00
51. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K121.259/0013-DSK/2007", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20070523_K121259_00013-DSK_2007_00
52. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K600.041-044/0003-DVR/2007", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20071003_K600041-044_0003-DVR_2007_00
53. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K120.790/010-DSK/2002", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKRS_20020903_K120790_010-DSK_2002_01
54. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K120.762/010-DSK/2001", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20011016_K120762_010-DSK_2001_00
55. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K121.200/0012-DSK/2006", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20061213_K121200_0012-DSK_2006_00
56. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K120.862/0011-DSK/2005", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20050520_K120862_0011-DSK_2005_00
57. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K121.392/0009-DSK/2009", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20090225_K121392_0009-DSK_2009_00
58. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K178.313/0005-DSK/2008", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20081022_K178313_0005-DSK_2008_00
59. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K178.328/0005-DSK/2008", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20081022_K178328_0005-DSK_2008_00
60. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K178.323/0005-DSK/2008", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20081022_K178323_0005-DSK_2008_00
61. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K178.303/0005-DSK/2008", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20080516_K178303_0005-DSK_2008_00
62. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K121.386/0009-DSK/2008", retrieved 2010-10-16;

http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20081022_K121386_0009-DSK_2008_00

63. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K121.313/0016-DSK/2007", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20071212_K121313_0016-DSK_2007_00
64. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K121.040/0018-DSK/2005", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20051216_K121040_0018-DSK_2005_00
65. Bundeskanzleramt Österreich, "Bescheid der Datenschutzkommission / Geschäftszahl K120.819/0006-DSK/2003", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20031114_K120819_006-DSK_2003_00
66. Bundeskanzleramt Österreich, "OGH RS0113731", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20000628_OGH0002_0060OB00162_00T0000_001
67. Bundeskanzleramt Österreich, "OGH RS0113740", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20000628_OGH0002_0060OB00148_00H0000_001
68. Bundeskanzleramt Österreich, "OGH RS0113846", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20000628_OGH0002_0060OB00148_00H0000_002
69. Bundeskanzleramt Österreich, "OGH RS0114317", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20001114_OGH0002_0140OS00128_0000000_002
70. Bundeskanzleramt Österreich, "OGH RS0114637", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20010130_OGH0002_0140OS00114_0000000_001
71. Bundeskanzleramt Österreich, "OGH RS0115217", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20010322_OGH0002_0040OB00028_01Y0000_004
72. Bundeskanzleramt Österreich, "OGH RS0116693", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20020613_OGH0002_008OBA00288_01P0000_000
73. Bundeskanzleramt Österreich, "OGH RS0116746", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20020903_OGH0002_0110OS00109_0100000_001
74. Bundeskanzleramt Österreich, "OGH RS0117271", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20021119_OGH0002_0040OB00179_02F0000_007
75. Bundeskanzleramt Österreich, "OGH RS0120087", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20050726_OGH0002_0110OS00057_05Z0000_002
76. Bundeskanzleramt Österreich, "OGH RS0120439", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20051215_OGH0002_0060OB00275_05T0000_001
77. Bundeskanzleramt Österreich, "OGH RS0120930", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20060629_OGH0002_006OBA00001_06Z0000_002
78. Bundeskanzleramt Österreich, "OGH RS0121196", retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20060914_OGH0002_0060OB00167_06M0000_001

79. Bundeskanzleramt Österreich, “OGH RS0123204”, retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20080207_OGH0002_009OBA00104_07W0000_001
80. Bundeskanzleramt Österreich, “OGH RS0124264”, retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20081001_OGH0002_0060OB00195_08G0000_001
81. Bundeskanzleramt Österreich, “OGH RS0124274”, retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20081001_OGH0002_0060OB00195_08G0000_002
82. Bundeskanzleramt Österreich, “OGH RS0124275”, retrieved 2010-10-16; http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJR_20081001_OGH0002_0060OB00195_08G0000_003
83. ARGE Daten - Österreichische Gesellschaft für Datenschutz, “ARGE Daten”, retrieved 2010-10-16; http://www.argedaten.at
84. A-SIT Zentrum für sichere Informationstechnologies - Austria, “Bürgerkarte”, retrieved 2010-10-16; http://www.buergerkarte.at
85. Bundeskanzleramt Österreich, “Datenschutzrat”, retrieved 2010-10-16; http://www.datenschutzrat.gv.at/
86. Wirtschaftskammer Österreich, “E-Rechnung in Österreich”, retrieved 2010-10-16; http://www.e-rechnungen.at/
87. Wirtschaftskammer Österreich, “E-Rechnung in Österreich”, retrieved 2010-10-16; http://wko.at/e-business/e-rechnung/start/start.htm
88. Wirtschaftskammer Österreich, “Firmen A-Z”, retrieved 2010-10-16; http://firmen.wko.at
89. Dr. Franz Schmiderbauer, “Vorratsdatenspeicherung ante portas”, retrieved 2010-10-16; http://www.internet4jurists.at/news/aktuell96a.htm
90. ”ECG-Liste”, retrieved 2010-10-16; http://www.rtr.at/de/tk/E_Commerce_Gesetz
91. RTR-GmbH, “Rundfunk & Telekom Regulierungs-GmbH”, retrieved 2010-10-16; http://www.rtr.at
92. RTR-GmbH, “Aufsichtsstelle für elektronische Signaturen“, retrieved 2010-10-16; http://www.signatur.rtr.at/
93. Sveriges riksdag, “Tryckfrihetsförordning (1949:105)”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1949:105
94. Sveriges riksdag, “Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1960:729
95. Sveriges riksdag, “Yttrandefrihetsgrundlag (1991:1469)”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1991:1469
96. Sveriges riksdag, “Lag (1995:1506) om hemlig kameraövervakning”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1995:1506
97. Sveriges riksdag, “Statens offentliga utredningar (SOU) 1997:39”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3281&dok_id=GLB339d2
98. Sveriges riksdag, “Lag (1998:112) om ansvar för elektroniska anslagstavlor”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1998:112
99. Sveriges riksdag, “Lag (1998:150) om allmän kameraövervakning”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1998:150
100. Sveriges riksdag, “Personuppgiftslag (1998:204)”, retrieved 2010-10-16; http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf, http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1998:204
101. Sveriges riksdag, “Personuppgiftsförordning (1998:1191)”, retrieved 2010-10-16; http://www.sweden.gov.se/sb/d/574/a/25633, http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1998:1191
102. Sveriges riksdag, “Lag (2000:832) om kvalificerade elektroniska signaturer”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2000:832

103. Sveriges riksdag, “Förordning (2000:833) om kvalificerade elektroniska signaturer”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2000:833
104. Sveriges riksdag, “Lag (2001:99) om den officiella statistiken”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2001:99
105. Sveriges riksdag, “Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2002:562
106. Sveriges riksdag, “Lag (2003:389) om elektronisk kommunikation”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2003:389
107. Sveriges riksdag, “Distans- och hemförsäljningslag (2005:59)”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2005:59
108. Sveriges riksdag, “Förordning (2007:975) med instruktionen för Datainspektionen”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2007:975
109. Sveriges riksdag, “Marknadsföringslag (2008:486)”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2008:486
110. Sveriges riksdag, “Offentlighets- och sekretesslag (2009:400)”, retrieved 2010-10-16; http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2009:400
111. Staffan Malmgren, “NJA 2000 p. 292”, retrieved 2010-10-16; https://lagen.nu/dom/HDO/B413-00_1
112. Staffan Malmgren, “Regeringsrätten 4174-00”, retrieved 2010-10-16; https://lagen.nu/dom/ra/2001:35
113. Staffan Malmgren, “Regeringsrätten 7517-00”, retrieved 2010-10-16; https://lagen.nu/dom/ra/2001:68
114. Staffan Malmgren, “Högsta Domstolen B293-00”, retrieved 2010-10-16; https://ferenda.lagen.nu/dom/nja/2001s409
115. Staffan Malmgren, “Regeringsrätten 4367-01”, retrieved 2010-10-16; https://lagen.nu/dom/ra/2002:54
116. Staffan Malmgren, “Svea hovrätt B4812-02”, retrieved 2010-10-16; https://lagen.nu/dom/rh/2002:71
117. Staffan Malmgren, “Göta hovrätt B747-00”, retrieved 2010-10-16; https://ferenda.lagen.nu/dom/rh/2004:51
118. Staffan Malmgren, “Regeringsrätten 2771-02”, retrieved 2010-10-16; https://lagen.nu/dom/ra/2004:104
119. Domstolsverket, “Högsta domstolen B1624-03”, retrieved 2010-10-16; http://www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2004/2004-11-08_B_1624-03_dom.pdf
120. Domstolsverket, “Högsta Domstolen B3042-03”, retrieved 2010-10-16; http://www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2005/2005-05-26_B_3042-03_Dom_skiljaktighet.pdf
121. Domstolsverket, “Högsta domstolen B2669-07”, retrieved 2010-10-16; http://www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2008/2008-10-23%20B%202669-07%20Dom.pdf
122. Domstolsverket, “Regeringsrätten 6588-05”, retrieved 2010-10-16; http://www.regeringsratten.se/Domstolar/regeringsratten/Avg%C3%B6randen/2008/December/6588-05.pdf
123. Marknadsdomstolen, “Marknadsdomstolen 2009:8”, retrieved 2010-10-16; http://www.marknadsdomstolen.se/avgoranden/avgoranden2009/Dom2009-8.pdf
124. Justitiekanslern, “Justitiekanslern Diarienr. 5532-09-31”, retrieved 2010-10-16; http://www.jk.se/Beslut/Tryck-OchYttrandefrihetsarenden/5532-09-31.aspx
125. Domstolsverket, “Regeringsrätten 1789-08”, retrieved 2010-10-16; http://www.regeringsratten.se/Domstolar/regeringsratten/Avg%C3%B6randen/2010/Januari/1789-08.pdf

126. Datainspektionen, “Datainspektionen Diarienr. 1020-2005”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2005-08-30-sl_skadegorelsedatabas.pdf
127. Datainspektionen, “Datainspektionen Diarienr. 764-2007”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2007-12-18-standard-poors.pdf
128. Datainspektionen, “Datainspektionen Diarienr. 473-2008”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2008-06-24-Soc-tanter.pdf
129. Datainspektionen, “Datainspektionen Diarienr. 685-2008”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2008-09-09-Uppsala.pdf
130. Datainspektionen, “Datainspektionen Diarienr. 767-2008”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2009-01-13-ving.pdf
131. Datainspektionen, “Datainspektionen Diarienr. 1476-2008”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2008-12-16-ica.pdf
132. Datainspektionen, “Datainspektionen Diarienr. 513-2009”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2009-12-21-pliktverket.pdf
133. Datainspektionen, “Datainspektionen Diarienr. 514-2009”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2010-03-01-busslink.pdf
134. Datainspektionen, “Datainspektionen Diarienr. 604-2009”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2009-12-14-kamera-matbutik.pdf
135. Datainspektionen, “Datainspektionen Diarienr. 987-2009”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2010-02-02-trelleborg.pdf
136. Datainspektionen, “Datainspektionen Diarienr. 1288-2009”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2010-01-12-rejtingsajt.pdf
137. Datainspektionen, “Datainspektionen Diarienr. 1837-2009”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2010-06-23-onoff.pdf
138. Datainspektionen, “Datainspektionen Diarienr. 685-2010”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2010-07-05-katrineholm.pdf
139. Datainspektionen, “Datainspektionen Diarienr. 686-2010”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2010-07-05-arbetsmiljoverket.pdf
140. Datainspektionen, “Datainspektionen Diarienr. 687-2010”, retrieved 2010-10-16; http://www.datainspektionen.se/Documents/beslut/2010-07-05-grona-lund.pdf
141. Svenska Antipiratbyrän, “Svenska Antipiratbyrån”, retrieved 2010-10-16; http://www.antipiratbyran.com
142. Piteå-Tidningen, “Bahnhof förstör Ipreduppgifter”, retrieved 2010-10-16; http://www.pitea-tidningen.se/nyheter/telegram/artikel.aspx?ArticleId=4569419
143. Finansiell ID-Teknik BID AB, ”BankID”, retrieved 2010-10-16; http://www.bankid.com
144. Datainspektionen, “Datainspektionen”, retrieved 2010-10-16; http://www.datainspektionen.se
145. Datainspektionen, “Förlängt undantag för Antipiratbyrån och IFPI ”, retrieved 2010-10-16; http://www.datainspektionen.se/press/nyhetsarkiv/2006/Forlangt-undantag-for-Antipiratbyran-och-IFPI–/
146. Datainspektionen, “Personnummer som änvänderidentitet vid inloggning”, retrieved 2010-10-16; http://www.datainspektionen.se/personuppgiftsombud/samradsyttranden/personnummer-som-anvandaridentitet-vid-inloggning-/
147. Datainspektionen, “Samrådsyttranden”, retrieved 2010-10-16; http://www.datainspektionen.se/personuppgiftsombud/samradsyttranden/
148. Datainspektionen, “Överföring av personuppgifter till tredje land”, retrieved 2010-10-16; http://www.datainspektionen.se/om-oss/internationellt-arbete/tredjelandsoverforing/
149. Datainspektionen, “Föreskrifter om ändring av Datainspektionens föreskrifter (DIFS 1998:2) i fråga om skyldigheten att anmäla behandlingar av personuppgifter till Datainspektionen”, retrieved 2010-10-16;

http://www.datainspektionen.se/Documents/datainspektionen-foreskrifter-2001-1.pdf

150. Bolagsverket et al., “e-legitimation.se”, retrieved 2010-10-16; http://www.e-legitimation.se
151. IFPI, “International Federation of the Phonographic Industry - Svenska Gruppen”, retrieved 2010-10-16; http://www.ifpi.se
152. Konsumentverket, “Konsumentverket”, retrieved 2010-10-16; http://www.konsumentverket.se
153. Radio och TV-Verket, “Radio- och TV-Verket”, retrieved 2010-10-16; http://www.rtvv.se/se/Internet/utgivningsbevis/
154. GEEP EDS LLC, “Darik’s Boot And Nuke”, retrieved 2010-10-16; http://www.dban.org
155. Jos Dumortier et al., “The legal and market aspects of electronic signatures”, Katholieke Universiteit Leuven, 2005, retrieved 2010-10-16; http://ec.europa.eu/information_society/eeurope/2005/all_about/security/ electronic_sig_report.pdf
156. Commission of the European Communities, “Europe’s Digital Competitiveness Report 2009”, retrieved 2010-10-16; http://ec.europa.eu/information_society/eeurope/i2010/key_documents/index_en.htm
157. Facebook, “Facebook”, retrieved 2010-10-16; http://www.facebook.com
158. Google, “Google Analytics”, retrieved 2010-10-16; http://google.com/analytics
159. Olaf Gutsche, “Die Umsetzung der E-Commerce-Richtlinie in der Bundesrepublik Deutschland und der Republik Österreich”, Jannuar 2003, retrieved 2010-10-16; http://iprserv.jura.uni-leipzig.de/magister/downloads/magisterarbeiten/Olaf_Gutsche.pdf
160. IEEE, ”Standard Specifications For Public-Key Cryptography”, retrieved 2010-10-16; http://grouper.ieee.org/groups/1363/
161. APM Group Ltd., “ITIL”, retrieved 2010-10-16; http://www.itil-officialsite.com
162. OGC, “ITIL V3 Small-Scale Implementation Book”, retrieved 2010-10-16; http://www.best-management-practice.com/officialsite.asp?FO=1253138&ProductID=9780113310784&Action=Book
163. Wikileaks, “British Telecom Phorm PageSense External Validation report”, retrieved 2010-10-16; http://www.wikileaks.org/wiki/British_Telecom_Phorm_Page_Sense_External_Validation_report
164. FreeRainbowTables, “Distributed Rainbow Table Project”, retrieved 2010-10-16; http://www.freerainbowtables.com/
165. SAP, “SAP”, retrieved 2010-10-16; http://www.sap.com
166. Bruce Schneier, “The Process of Security”, retrieved 2010-10-16; http://www.schneier.com/essay-062.html
167. Schoderbek et al., “Management Systems, 4th edition”, Richard D. Irwin Inc., 1990
168. Louis H. Sullivan, “the tall office building artistically considered”, 1896, retrieved 2010-10-16; http://academics.triton.edu/faculty/fheitzman/tallofficebuilding.html
169. TrueCrypt Developers Association, “TrueCrypt”, retrieved 2010-10-16; http://www.truecrypt.org
170. Sanna Wolk et. al., “Ownership of the Copyright in Works and the Patent Right in Inventions Created by Employees in Finland, Sweden, Germany, Austria, the United Kingdom, Estonia and Argentina“, Stockholm, 2002, retrieved 2010-10-16; http://www.juridicum.su.se/user/sawo/Publikationer/Wolk%20nr%20120.pdf
171. Craig Wright et al., “Overwriting Hard Drive Data: The Great Wiping Controversy”, Springer-Verlag Berlin Heidelberg, 2008, retrieved 2010-10-16; http://www.springerlink.com/content/408263ql11460147/
172. Xing AG, “Xing”, retrieved 2010-10-16; http://www.xing.com
173. Chaim Zins, “Conceptual Approaches for Defining Data, Information, and Knowledge”, retrieved 2010-10-16; http://www.success.co.il/is/zins_definitions_dik.pdf

Chapter 10
Indices

List of Figures

List of Tables

Chapter 11
Abstract (English)

The European Union strives to unify the legal situation in regard to data processing in Europe. This is done through directives, which then have to be implemented into national law. As a result of this process the local legal situation varies among the member states. This introduces additional hurdles for small to medium sized companies who operate across borders, apart from their already existing struggles to comply with their local legal requirements.

This thesis describes for Austria and Sweden the legal regulations that apply to a company handling information. Special emphasis has been given to practical examples and court decisions to point out the legal pitfalls in processing information by electronic means. The analysis focuses on processing business information between two entities as well as using information technology for internal purposes.

After introducing the legal situation, the second part of the work describes how a company can approach the issue at hand. By using a theoretical model the possible information flows and connections are shown and how they are affected by the legal requirements. Practical solutions are then provided and the differences in their implementation in Austria and Sweden are pointed out.

The thesis concludes with a high level comparison of the situation in the two countries, and general advice about which data protection philosophy a company should chose for each of them.

Chapter 12
Abstract (German)

Die Europäische Union strebt danach die rechtliche Situation für elektronische Datenverarbeitung in Europa zu vereinheitlichen. Dies geschieht durch Direktiven welche dann in nationalen Gesetzen implementiert werden müssen. Als ein Effekt dieses Prozesses variiert die lokale rechtliche Situation in den Mitgliedsstaaten. Dadurch entstehen zusätzliche rechtliche Hindernisse für Klein- und Mittelbetriebe welche über Landesgrenzen hinweg operieren, zusätzlich zu deren bereits bestehenden Anstrengungen die lokalen Vorgaben zu befolgen.

Diese Arbeit beschreibt für Unternehmen in Österreich und Schweden die rechtlichen Vorschriften hinsichlich Informationsverarbeitung. Besonderes Augenmerk wurde auf praktische Beispiele und Gerichtsurteile gelegt, um die rechtlichen Fallstricke im Rahmen der elektronischen Datenverarbeitung aufzuzeigen. Die Analyse konzentriert sich auf die Verarbeitung von Geschäftsinformationen zwischen zwei Parteien sowie die Verwendung von Informationstechnologie für interne Zwecke.

Nach der Darlegung der rechtlichen Situation beschreibt der zweite Teil der Arbeit wie ein Unternehmen an diese Probleme herangehen kann. Mittels eines theoretischen Modells werden die Informationsflüsse und Verbindungen aufgezeigt, und wie sie durch die rechtlichen Anforderungen betroffen sind. Praktische Lösungen werden dargelegt und deren Unterschiede in der Implementierung in Österreich und Schweden hervorgehoben.

Die Arbeit schliesst mit einem generellen Vergleich der Situation in beiden Ländern, und Hinweisen darüber welche Datenschutz-Philosophie ein Unternehmen jeweils wählen sollte.

Chapter 13
Curriculum vitae

Robert Hoffmann, a9502439@unet.univie.ac.at

Education

2010 - 2011	Master program “Information and Communication Systems Security” at the KTH Royal Institute of Technology, Stockholm * Thesis: “A holistic evaluation of information security metrics”
2009 - 2010	Exchange student (Erasmus) at the University of Stockholm, Institutionen för data- och systemvetenskap (DSV)
2006 - 2010	Master of Science in “Business Informatics”, University of Vienna * Specialization on IT security * Thesis: “The European data protection laws and their practical application in Austria and Sweden”
2006 - 2009 and 1995 - 2000	Bachelor of Science in “Business Informatics”, University of Vienna * Specialization on business process design and usability
2008	IPICS Rovaniemi, Finland
2008	Training as data protection officer in Austria
2005	Six Sigma Green Belt certification
1989 - 1994	High school for IT and organization, Villach, Austria (HTL für EDV und Organisation)

Employment History

2011	Student assistant at the KTH Royal Institute of Technology
2001 - 2010	IT specialist, Honeywell Austria GmbH
2008 - 2009	Tutor at the University of Vienna
1999 - 2001	IT trainer, Venetia GmbH
1998	IT consultant, BOC AG
1996 - 2002	IT administrator, student hostel “Haus Döbling”