School of Economics and Commercial Law
GÖTEBORG UNIVERSITY

SECURING OWNERSHIP OF INTANGIBLE ASSETS IN A SUBJECT BASED NETWORK

Gothenburg School of Economics and Commercial Law
Department of Law
Final Thesis

40 Credits

Annette Utternäs,

Björn Johansson

Tutor: Ulf Petrusson

1. Subject

The subject of this thesis is to investigate how a production company that has organized its sales network with independent retailers, thus creating a low vertically integrated value chain, may secure ownership to an object that is claimed by many actors within the network. The object that we are investigating how to secure, is personal data that is collected from customers and potential customers that come in contact with the producing company via different channels. Personal customer data that is well organized in a customer database, may create great financial value as it creates a link to individuals interested in the company, and therefore may improve the relations with existing and potential customers. As the value of the customer data is discovered the independent retailers may be protective of the personal data that they collect as there may exist competition between different retailers within the same region, which could create difficulties for the production company to convince the retailers to hand over the customer data. This may create problems to create effective direct marketing campaigns, as the producing company's customer database only may contain a fraction of all the personal data that has been collected in the entire network.

Another issue is to make sure that all personal data is collected and processed in a way that complies with personal integrity regulations. This issue becomes even more complicated as many companies are active in the global arena where the regulations may differ from country to country. To handle the personal data in a correct manner is extremely important as it may not only create legal issues but also public "bad will" if the personal data is processed in a reckless way. This could create the opposite result to the purpose of collecting the data and would make the customer database worthless. To avoid this scenario a company needs to create a personal data usage policy that clarifies the company standpoint regarding personal integrity and the customer database, and how the personal data shall be processed within the network.

The handling of the customer database and the personal data that it contains must be seen as one of the most important processes in a company today, thus this thesis shall only be seen as a beginning towards understanding how important and complex the issues really are.

2. Method

When starting to investigate the subject of this thesis, we discovered that there was a great deal of complexity involving the situation. We realized that it is not enough to understand one issue at a time, but also how the issues connect and interact. As most companies quite recently have started to discover the potential of their customer databases, if not yet their full potential, there is not very much written in this area. The conclusions that we have come to are the result of literary studies, interviews with employees from Volvo Car Corporation, the Data Inspection Board (both in Sweden and corresponding authorities in other countries), Domain Network and most of all endless discussions with researchers and colleagues at the Center for Intellectual Property Studies, Chalmers University of Technology and the Department of Law, Gothenburg University. Our main focus has been to find possibilities instead of problematic interpretations of the legal framework and to at all times keep a business focused perspective. This essay shall in no aspect be seen as a suggestion of a full strategy or an answer book but merely as a study of how a company could structure, relate to and govern its customer database to be able to consider it as property and by doing this secure both the customer data and the database structure.

3. Introduction

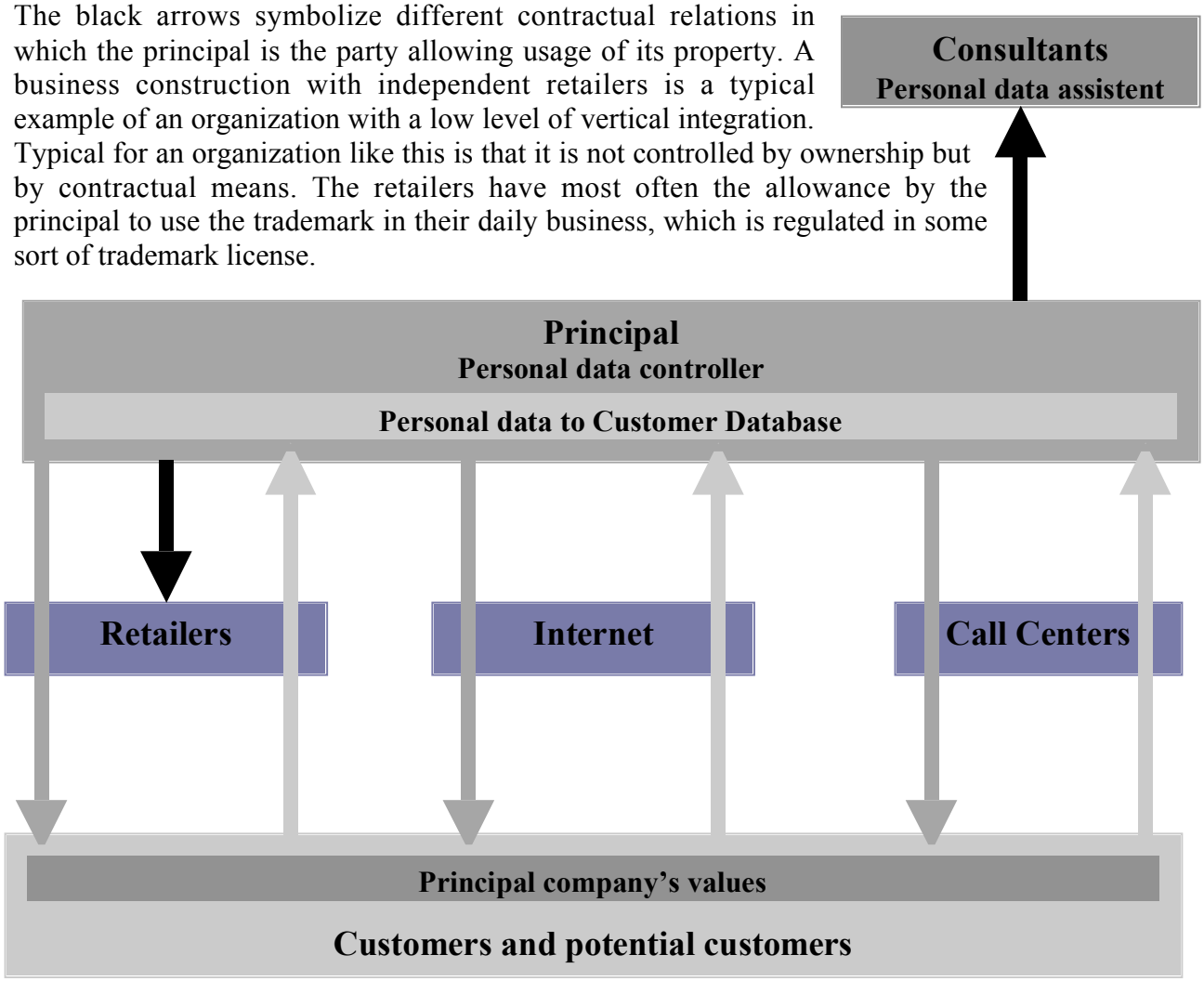
In the old economy a production company simply sold products but today that is not enough. To be able to survive and be successful in an environment of ongoing globalization and the increased competition that follows, a company must be able to communicate that it is not only selling a product but also values that are connected to the product, the use of the product and the trademark in itself. The need for having a competitive edge is essential. To reach, attract and maybe the most important, to keep customers and communicate the company's values such as responsibility for health, environment and ethics have become the greatest challenges in the new economy. To be able to do this the customers need to be closely attached to the company so that the company has en opportunity to nourish the customer relations and differentiate the marketing effort depending on the segment of the market that the company is aiming for in different situations.

Modern technology has provided companies with a powerful tool to achieve these objectives. A database, as a systematically arranged collection of computer data, structured so that it can be automatically retrieved or manipulated, can store millions of customers and their personal data, and the information can be distributed over the world in just a couple of seconds. A multinational company can use this tool to create a very powerful competitive advantage by harmonizing customer knowledge and relations, thus creating synergy both in the form of cost savings and by creating value. However, many companies are organized in widely spread networks of actors that are not controlled by the mother company through ownership, but still closely related to and cooperating with this principal. When creating the necessary subject based structures the relations therefore need to be strictly regulated to avoid any issues or such conflicts that may arise as the network on different levels creates business values. As the value of a company today becomes more and more dependant on values and intangible assets, the success of a company to a greater extent relies on how it can protect, govern and communicate these assets. The concrete problems that many companies face regarding customer relations in general and customer data in particular, are the questions of customer integrity and ownership to said customer data, as regards other actors within the business network. To be able to create and maintain a win-win situation within this collaboration between subjects, such as the mother company, business partners and customers, the legal tools must be used to create the best possible value for all subjects involved. At the same time it must ensure that the property that is being created is structured, regarding first of all ownership, but equally important how subjects other than the property holder, may use the property to enhance its value. In the future the company that succeeds in building a structure of contractual relations has the best opportunities to become more profitable. This is best accomplished with awareness of the complexity involved in these matters. It is important to remember that these are early days still in most companies and society as such, when it comes to fully comprehending the concept of intellectual property and intangible assets and their function and full potential. Realizing the need for an understanding of this complexity is probably the first and most important step and can certainly give a company a head start. However; an even more prosperous future and development can be expected for the ones that consider this an ongoing process and are ready and willing to take on the challenge leveraging their intangilble assets

The figure below shows the different relationships between different actors that may be involved in the collection of customer data. The light grey arrows symbolize the personal data that is being collected. The dark grey arrows symbolize the values that the principal sends out through their trademark via different channels such as retailers, the Internet and call centers.

Common for these channels is that they should only be seen as a means for the principal to reach the customers and potential customers and for the personal data to be transferred to the rightful owner, which is the principal due to the trademark and their investment in this process as this is what attracts customers in the first place.

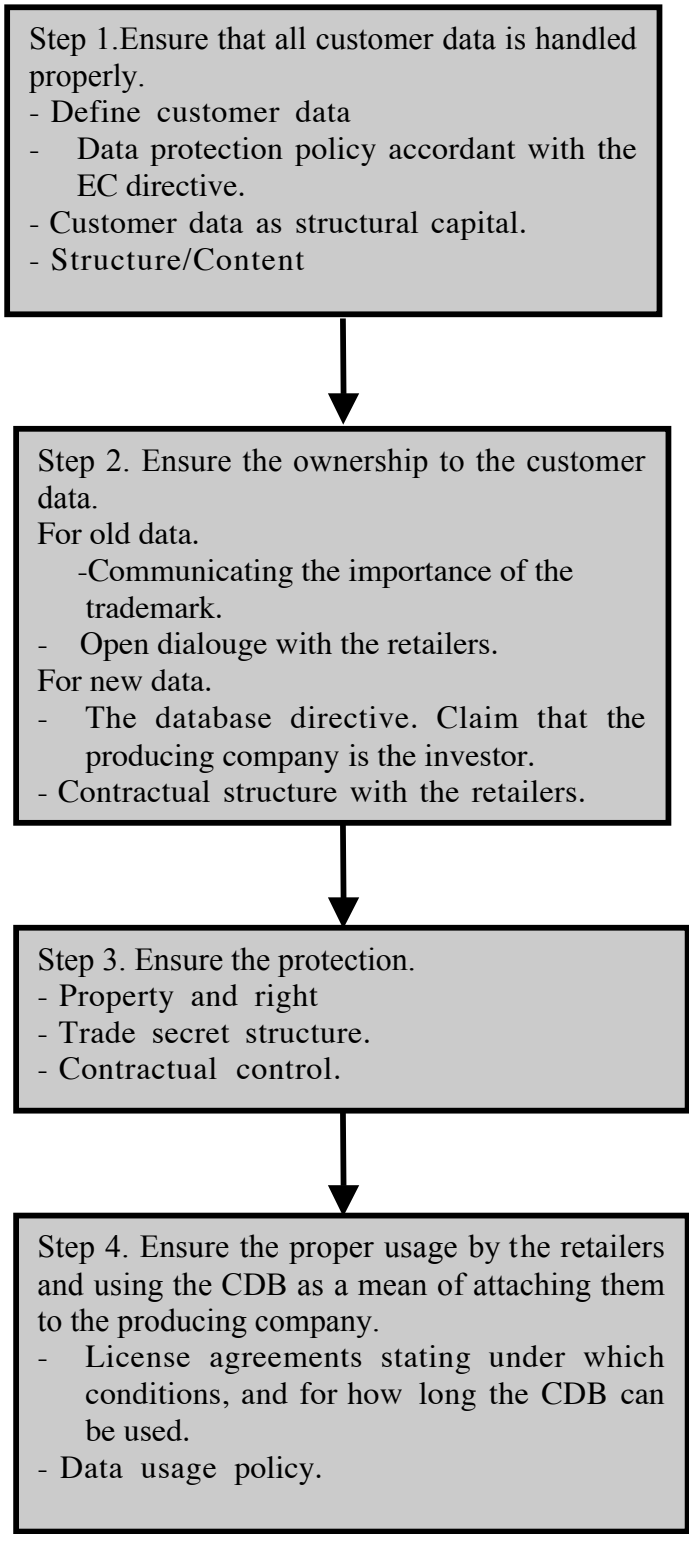
The black arrows symbolize different contractual relations in which the principal is the party allowing usage of its property. A business construction with independent retailers is a typical example of an organization with a low level of vertical integration. Typical for an organization like this is that it is not controlled by ownership but by contractual means. The retailers have most often the allowance by the principal to use the trademark in their daily business, which is regulated in some sort of trademark license.



Once the control of the personal data is secured, it can also be the object for a license construction, in form of a database usage license agreement. As the retailers will be personal data assistants according to PUL, this also needs to be regulated.

Different consultants and business partners may use the personal data, for example to create marketing campaigns for the principal. These actors must also be contractually connected to the principal so that they can be allowed to process the personal data.

This flowchart describes from an overview perspective the necessary considerations that a company needs to take when processing customer data and governing a customer database



4. The concept of property

This section will from a theoretical point of view describe the concept of property and why it is important for a company to by itself define what it considers to be its assets. As many of a company's prime assets today are of an intangible nature the company must by itself define and create structures for protection and governance of their property, using existing legal instruments as well as contractual strategies.

Society is built on perceptions of reality; perceptions that constitute what we as a community believe to be the one and only truth. Knowledge is something we all possess, but it is not always obvious what is knowledge and what is comprehended as knowledge.[1] This is the case also in the legal reality that companies are striving to comply with when conducting their business. Often you find that the law surrounding your business activities does not cover new business methods, and lawyers and business people struggle to make new situations fit into old and well-known legal concepts. With this understanding, a company has the possibility to create its own reality by building their own structures designed to create business value. The companies that are going to be successful in the future are the ones that can communicate their perceptions on what the reality consists of, and by doing this, creating a control position that allows them to influence their own future. New phenomena in a new time and in a new economy can be treated, handled and communicated in a way that others can accept and thereby create another set of perceptions that becomes the new truth. Relations to customers and information on customer habits and preferences are important issues for any company, and even more today since the Internet has made almost every company a world wide actor. This customer relation is one important structural brick, and companies that are aware of the fact that it is an asset (and preferably the full potential of several other intangibles within the company), will develop a competitive edge that is crucial today. [2]

In the area of intellectual property the perception can and must be divided into two different conceptions. One subject oriented, which pertains to the parties involved in the process, and one object oriented. When handling customer databases the company has primarily two kinds of subjects to handle; the customers, whose data is being stored e.g. the customer relations, and the subjects that shall be entitled to use the customer database, such as the company processing the data as well as business partners and retailers that may be entitled to use the data for marketing activities. Customer relations as such may seem difficult to make fit into a specific legal concept, but that to is a question of perceptions of what the reality actually is. A company can most certainly create structures that will make it possible to claim ownership to a customer relation. When handling intellectual property a company must also be aware of the concept of property. In order for it to be accepted, the customer relation needs to be in some kind of property form - it has to be objectified. This leads us over to the concept of an object, which in our case consists of the customer data as such, and the customer database. The customer database is, as we will explain later in the thesis, an object with legal property rights attached; and explains why the perception is that a customer database is a legally protected object. This will strengthen the perception that the customer relations, as the result of the company's business activities, will be property as well.

[1] Barlebo Wenneberg, Sören, "Socialkonstruktivism – positioner, problem och perspektiv"
[2] Petrusson, Ulf; "Patents as Structual Capital"

4.1. Tangible and Intangible assets from a legal perspective

The assets in a company can be divided into tangible and intangible assets. It is important for a company to distinguish between them and be aware of their differences, as it creates an understanding for what is or can be legally protected and how to achieve the protection. One must always remember that even if an asset is intangible, it is still a property that is important to structure and define to create ways to protect and govern it, and also to be able to value it in case of a transfer.

According to some authors an intangible asset must possess a number of characteristics to be considered an intangible asset.[3]

It should be subject to specific identification and recognizable description.
It should be subject to legal existence and protection.
It should be subject to the right of private ownership, and the private ownership should be legally transferable.
There should be some tangible evidence or manifestation of the existence of the intangible asset, for example a contract, a license a computer disquette, etc.
It should have been created or have come into existence at an identifiable time or as the result of an identifiable event.
It should be subject to being destroyed or to a termination of existence at an identifiable time or as the result of an identifiable event.

From this list you can easily draw the conclusion that it is essential to use legal tools, not only to protect the intangible asset, but also simply to bring it into existence. This fact together with the fact that we are handling a rather new area of business, can often give the impression that we are handling a situation of chaos, due to the lack of regulations that can be applied on the new phenomenon that the technology creates. This may to some extent be true, since the legal framework reflects reality and often comes second in time to the issues that may occur. However, there are applicable regulations in the area, both old that are important and require consideration, and new that have been created to govern new situations. One must not forget that the uncertainty creates golden opportunities for the company that is well prepared. As long as the company's actions are in line with what present regulations state, the company can itself create legal structures and policies that not only will be accepted by the community, but also will help the company to establish an effective and lucrative business environment.

The lack of strict external legal guidelines combined with an awareness of the existing regulations and good prognoses concerning the future regulations can be used to set up an internal legal structure.

When defining an intangible asset, one must first consider the fact that what is being discussed is in fact a kind of property, and must be subject to the rights of property.[4] The ability to *identify the asset* is essential to being able to treat the asset as property. One must aim for a clear and precise description that will identify the intangible asset as a unique piece of property, and it must enjoy the characteristic legal rights that come with property in general. The objective is to define a property in order to claim ownership.

The ownership also inflicts responsibilities on the owner, and is why it is important to be aware of your actions. As for customer databases, it is important, both legally and in regard to

[3] Robert F. Reilly, Robert P. Schweihs, Valuing Intangible Assets, McGraw-Hill 1999
[4] a.a s. 5

public goodwill, that it is in line with the regulations on personal integrity and ethical guidelines concerning what can be collected, processed and how the information can be used. The customer database will be used for several purposes and by many different company employees. Without internal policies and ethical guidelines for how it shall be treated by employees, the company can find themselves in legal difficulties as well as create bad will in the market.

The distinction between tangible and intangible assets is not as obvious as one would think. Consider a common definition of tangible assets as shown below.[5]

A tangible asset should have physical existence and substantial form; it should be corporeal.
A tangible asset should be capable of being touched and seen.
A tangible asset should be perceptible to the touch; it should be tactile.

The definition leads to confusion as one of the conditions of an intangible asset is that there be some tangible evidence of its existence. It can for example be a computer, diskette, license contract or a patent application that is visable and touchable in the same way as a truck or a piece of machinery. Tangible media is essential for the existence of an intangible asset. Without some form of tangible existence an asset is of no use and has no value.

Another way of describing the distinction between tangible and intangible assets is that:

The value of a tangible asset is created by its tangible nature.
The value of an intangible asset is created by its intangible nature.

What give the tangible asset its value are the tactile, corporeal and visual elements. For an intangible asset the tangible media is only the bearer of the value. The intangible assets' value comes from its intangible nature and the legal property rights associated with the ownership of the intangible asset. These rights include the right to exclude others from exploiting, commercializing, selling, leasing, licensing, using, and transfering the intangible asset.

In summary; the value of an intangible asset does not come from the piece of paper it is written on or the disquette that it is saved on. Its value comes in a large part from the property rights associated with its intangible value. Once again this fact states just how important it is for a company to be aware of the legal environment surrounding the ability to protect, govern, structure and control the intangible assets.

After realizing that both the subject, in form of customer relations, and the object, in form of the customer data and customer database, can be considered property, the question arises in relation to whom the concept of property should be used. Who is the owner and in control? The answer to this question must take its starting point by describing how it has been made possible to collect the customer data in the first place. The reason is that customers and potential customers have come in contact with the company because of their products and values that the company communicates through their *trademark*. This means that the trademark, as a bearer of values and visions, should be the true property holder over the customer relations and data. As a trademark of course cannot be the legally accepted property holder of anything the true owner becomes the holder of the trademark. The fact that the customer relations and customer database was built at all is due to the trademark as a communicative tool, thus the *practical* way of building the customer relations and customer database is of no importance. It would have been impossible *without* the trademark. No

[5] a.a s. 10

matter what kind of sales network and different contractual relations a multi national company wishes to set up, the trademark stays with the product. This is an example of how a company's intellectual property and intangible assets interact and create synergy effects. Although they need to be considered as separate assets, they are more valuable when they co-operate.

Structuring a customer database must be seen as an ongoing process, where the customer relations and the personal integrity at all time must be in focus. This must be done in combination with protecting the property that the database constitutes.

4.2. Customer relations

The characteristic about customer databases is that as intangible assets they are only a tool for a company to be able to achieve and use another intangible asset, which is the *relation to the customers*, potential or existing. The data base is therefore only of value as long as this relationship is built on a positive feeling for the company, which can be achieved by marketing quality products under a strong brand, ethical and environmental considerations and so on. The positive feelings of potential or existing customers towards the company creates an intangible asset, whose value is reflected and can be used in the database. The value of the database is only as great as the other tangible and intangible assets make it.

As for a production company, such as a car selling company, the feeling the consumers get from the tangible cars and the values that the company represents due to marketing and public relations through their brand, creates a value in the customer database as long as the customers are satisfied with the cars and associate them with a positive feeling attached to the brand. The customer database can then be used to uphold this feeling by keeping the customers satisfied. The feeling of being selected after directed marketing activities will create loyalty and mouth-to-mouth goodwill, and of course also possibilities to come in contact with potential customers.

Unfortunately many companies today look upon their intangible assets, such as brand, customer satisfaction and customer databases as one subject, instead of dividing them into different assets all protected and attached by legal rights. By differentiating the intangible assets, a company can protect each one of them and build a structure that binds them together in a flexible and useful portfolio where the intangible assets interact with each other.

By doing this the company will also be able to locate where in the structure ethical and legal problems may arise. The internal structure can be built to first of all prohibit unwanted issues from arising. Secondly; if they occur, how to handle them in the most effective and safe way, without letting the problems contaminate the other intangible assets. As stated above, a customer database that is handled carelessly can cause ethical and legal difficulties that will effect customer relations as well as generate bad will for the brand.

4.3. Customer and business partner relations as intangible assets.

The most obvious criteria for determining whether a company is going to be successful is that it has customers that buy and appreciate the company's products. This is closely attached to the concept of trademarks as a trademark simply can be described as a tool to represent and transmit the company's values and standards. The value of the trademark is built on what kind of feelings and perceptions it conveys to the consumers. Without positive customer perception a business or trademark is worthless. However, as customer relations are essential to create a value for the business and trademark, customer relations also become an intangible asset themselves. A company must find the structure that enables their appreciation as such and in

the same time take advantage of their entire value. This can be achieved by creating a proper *contractual structure*.

Intangible assets are often the result of the work of company employees. The employee's competence, skill, talent and knowledge that is the foundation of intangible assets are what is referred to as the companies' human capital. Human capital is by many companies considered to be inseparable from the individuals, meaning that if an employee leaves the company she takes the human capital with her. And yes, fo*r human* capital this is true, as human capital only exists in the form of a human being. From the company's perspective it is therefore important to attach the knowledge in the form of human capital into the company structure where it becomes structural capital, which is the part of the knowledge structure that is attached to the company. When transforming the human capital into structural capital you start to objectify the knowledge, with the result that it can be of use for the entire company even if the employee chooses to end her employment. By treating any such new structural capital as property, a new intangible asset has been created.

For example; Employees gains know - how in a research process, which is transformed from human capital into structural capital in the form of patents and trade secrets owned by the company.

Knowledge about customers can be looked upon in the same way. It also needs to be transformed into a larger structure, such as a customer database so that it can be seen as structural capital, which can be of use, if governed properly, for the whole company and its business activities. The difference between the intangible assets with a longer history of acceptance and therefore a more mature social understanding such as patents and copyrights, and new intangible assets such as customer relations is that the company by itself must start to create an acceptance of the concept. A large company can by itself change the society to accept new forms of intangible assets and by creating new business structures within the company, and in the society as a whole, and by doing this enhance the protection of its intangible assets as its social understanding matures. To achieve this a company must be aware and establish an understanding of the existing legal tools as well as how they can be used for the company's objectives.

The concept of a customer database can be seen from two perspectives. It can be seen as an intangible asset in itself, encompassing the personal data from existing customers and potential customers, or it can be seen as a mean of enhancing the relations with the customers. It is therefore possible to consider the customer relations themselves as an intangible asset and as such being a part of the structural capital in the company. Furthermore; to enhance consumer relations the company must not only take care of the data derived from already existing customers, but also from potential customers that come in contact with the company in its daily business. The company needs to develop a strategy that makes it possible to structure and use this personal data. It is a question of objectifying customer knowledge and, by doing so, creating property. The perception of it as property can be enhanced by a licensing construction with actors that should be entitled to use the knowledge about the customers.

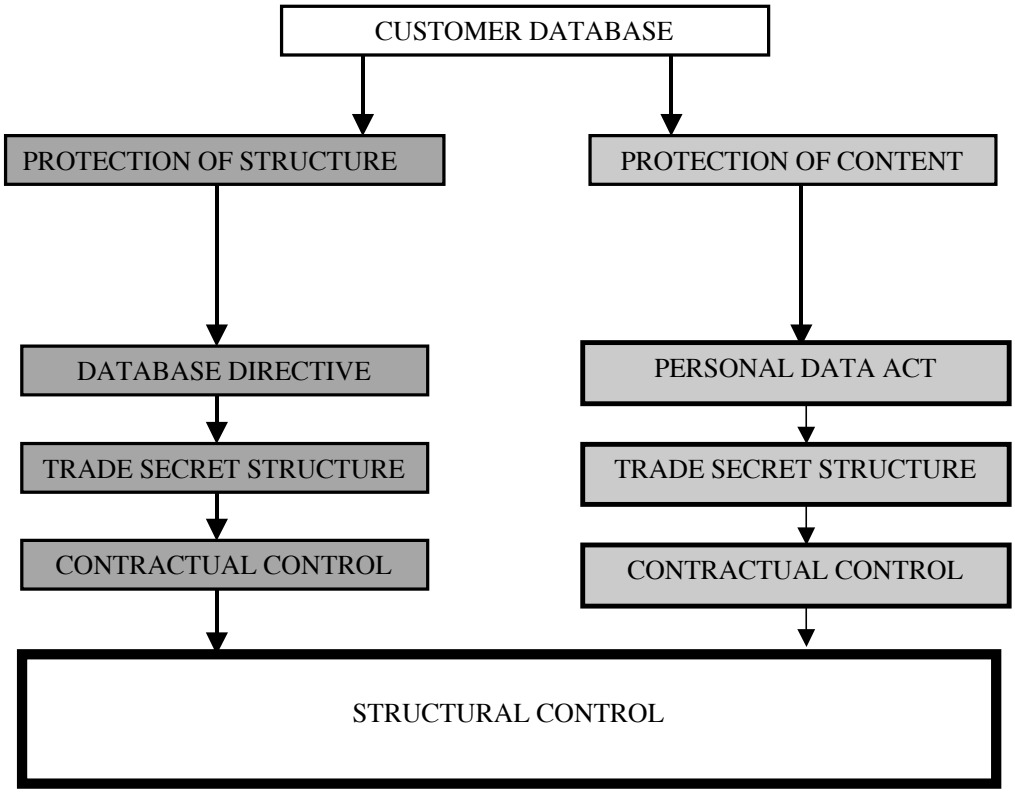
5. The Customer database

This section will start to describe the characteristics of a customer database and explain the differences from a legal perspective between the database structure and the database content. It will also describe the different legal tools that a company may use to secure both of these assets.

A company's customer data is maybe one of its most important assets and it is necessary to be familiar with the concepts of *structure* and *content* in order to secure the value of this customer relation. Legal tools can be used to build, control and protect both the structure and the content separately. By such legal actions it is possible to attain the main objective, which is to enhance customer relations and protect the structural capital the company is building.

The *content* in a customer database consists of the personal data that is being processed. Such information can be misused from a personal integrity point of view, why the legislator has found it necessary to create rules to ensure every individual's privacy. A company that wishes to use personal data must comply with existing regulations so they do not build the structure with illegal content. Furthermore it is important that the content is protected from infringement.

The collective personal data and the actual database technology constitute the *structure* of the customer database, and this requires different legal protection**.**



5.1. Securing the content

Industry has today more easily, due to the Internet, access to a global market. Potential customers can be reached instantly with adjusted offers. This is a great advantage and many companies are creating customer databases and consider them a major corporate asset. It is therefore of utmost importance that management is aware of what to consider when *processing* personal data, in order to comply with legislation, and that this is communicated and implemented to the operational level of the company. The law, however, does not regulate in detail what can be done and what cannot be done. The legislator is not as imaginative as people with marketing skills, naturally, and would of course not be able to cover all possible market measures they might suggest. The legal framework concerning the area of processing personal data is therefore designed to provide a protection for private persons integrity as such.

5.2. Processing of Personal Data

5.2.1. Personal integrity

As society and technology are changing rapidly the need for enhanced security for individual's privacy increases. Many countries have lately reviewed their legislation in this area and introduced new adjusted and improved acts. The aim is to protect personal integrity in the information society without unnecessarily preventing or complicating the use of new technology. The right to make documents public and official is considered an element of freedom of press, according to Swedish constitutional legislation, Freedom of the Press Act, 1:1 (1949:105). The principle of Public Access to Official Records (Offentlighetsprincipen) 2 Chapter, same act, does not restrict the availability of public documents even when the purpose is not for the freedom of the press explicitly. The right to public access to official records is regardless of purpose. The consequence of this interpretation of constitutional rights is not only that this legislation acts as a guarantee and control of the authority's work and actions for private persons and media, but also that personal data can be made available for commercial interests. The right to public documents is therefore not without restrictions. In consideration of other opposing interests, such as personal integrity, certain exemptions are regulated in The Secrecy Act (1980:100). As for the permitted processing of data, it is regulated in The Personal Data Act (1998:204), based on the EC Directive 95/46/EG.

5.2.2. EC directive

The EC directive 95/46/EG, on protection for private persons regarding processing of personal data, was approved 24 October 1995. The purpose of the directive is to create a common and high level of protection for personal integrity to facilitate a free flow of personal information, within the European Union. Sweden has implemented the directive and it has become national law as Personal Data Act (1998:204), which also replaced Data Act (1973:289). [6]

The directive is applicable on all processing of personal data, both automated and manual processes. Processing of personal data regarding public and state security, criminal law, personal use, journalistic work, art and literature is exempted.

[6] Prop. 1999/2000:11

Personal data may only be processed for specific and explicitly stated and authorized purposes, and may not be used at a later stage for inconsistent purposes.

A company must clearly state the purpose for the processing of the personal data, to the private person in question.. An example of how a company otherwise may damage its business is ”Let’s buy it” who intended to sell their database at a high price. It was then found out that a transaction of the database would be illegal, due to the fact that selling it was not a stated purpose. As ”Let’s buy it ” became bankrupt, the database therefore had no value, since the bankruptcy estate could not sell it either.

Consent must be obtained, for processing of personal data unless it is necessary to fulfill an agreement to which the registered is a party, or in order to perform obligations according to law or to protect a private persons fundamental interests. Processing of personal data may also take place if all interests have been weighed and balanced and the result is that processing is necessary.

It is allowed without consent to process personal data, related to a buyer of a car, as long as the processing is necessary for the purchase of the car, for example to be able to inform the customer about detected errors in a special model.

Sensitive personal data is information regarding a private person’s ethnic background, religion, political and union affiliation, sexuality and state of health. Such sensitive information may not be processed, unless consent has been given. Necessary handling for health and medical service is exempted.

The registered person shall receive information on who is responsible for the register and to what the information shall be used and has the right to have his right tried and protected by the national legal system.

The information shall be given at the same time as the registeree agrees to to have his personal data processed.

Transfer of personal data to a third country, may only take place if the country offers adequate level of protection for personal data.

The Datalags-committee, composed by the Swedish government in June 1995, proposed a Personal Data Act that regulates what is *permitted* regarding processing of personal data, as opposed to what is *forbidden*. It mainly follows the text and structure of the directive.

5.2.3. Personal Data Act

The Personal Data Act (1998:204) came into force 24 October 1998, and thereby replaces The Data Act (1973:289). It aims to protect all individual's privacy and protect personal integrity when processing personal information, both automatically and manually. Every violation may lead to claims for damage and in some cases even lead to penalty. [7]

The EC directive 95/46/EC, as of 24 October 1995, laid the groundwork for this new legislation, and Sweden may not have more rigid or more lenient regulations than the directive. The Personal Data Act includes, more or less, the same regulations as the directive and follows the same structure and text. Words and expressions are to have a common signification and if the meaning is indistinct, Swedish courts shall ask the **EC court** for advance notification. They have exclusive competence to interpret EC law. Since EC directives are without preparatory work, there are no guidelines for interpretation, except for the preamble and the text itself, and no practice is yet established.

The Personal Data Act is constructed with the same restrictive technique as the directive, meaning that all processing is forbidden as a main rule and the exemptions are then stated. If there is no legal authority to be found in the law, the processing is forbidden even if no violation of personal integrity is involved.

The purpose of the directive is to attain a free flow of personal information between the member states. However; according to Swedish constitutional law, every citizen shall receive protection against violations of his or hers personal integrity. The Personal Data Act states how this shall be achieved. Regarding IT business the act shall be applied by *all professional computer users* in Sweden today and the act gives rights to *every private person* whose information is being processed.

The Personal Data Act is subsidiary in relation to other constitutions. Other laws and regulations that states different, shall be applied instead. Rules that stipulate that public authorities may or shall hand out public documents, according to Offentlighetsprincipen, is one such example. However; directions issued by public authorities, such as the Data Inspection Board, have no priority over the Personal Data Act.

5.2.4.Processing of personal data

All kinds of processing are covered. This includes every measure or series of measures that is taken, concerning personal data, whether automated or manual, such as collecting, registration, organization, storage, arrangement or correction, recovering, obtaining, usage, distribution by sending, diffusion or any other disposal of data, compilation or co-ordination, blocking, obliteration or destruction.

For automated processing it is not necessary that the personal data is organized in a register of some kind. According to the Datalags-committee it is clarified that processing in computers in a computer format, in binary form as ones and zeros or similar, and transfer of personal data into such format, is considered automated processing. As soon as personal data has entered into a computer, it is a question of such automated process.

Partially automated processing is also included. For example if a computer index is connected to paper documents, with references that makes it possible to identify individuals.

[7] The examination and description of the Personal Data Act is based on: Öman/Lindblom, PersonuppgL – en kommentar

All computer processing of personal data in running text or in the form of pictures of individuals or pictures of text regarding individuals is included. The entire scope may not be ascertained at this stage, since no practice on the area is established.

5.2.5. Personal data

All information that *can* be assigned to a private individual is considered to be personal data. Examples on personal data are, name, personal code number, customer number, citizenship, shareholding and employment. The relevant circumstance is that one, specific physical person can be identified by the information.

To have any use of the processed data, it is most often important that a specific person can be identified. Almost every data regarding customers that a company processes are therefore often considered personal data.

The Personal Data Act is applicable also on encrypted data, as long as someone can make the data into readable form and by that identify individuals, direct or indirect. Also IP addresses and other electronic identities that could be collected on the Internet are covered by the act, since information assigned to a physical individual often can be found, via the ISP.

The definition of registered means that personal data on deceased or the unborn is not included. The purpose of the act is to protect personal integrity where it is most explicit, meaning for persons who are alive and can have a claim on such integrity. Data on a deceased person may be included if such data, direct or indirect, can be assigned to any other living person.

For legal entities, data is not included, even if a physical person owns it or it is named after a physical person. Private firm (enskild firma) data is included, since a physical person always is the owner. All data that can be assigned to a specific, physical person is included, even if the information only relates to the person as practicing a profession or being a businessman.

5.2.6. Controller of personal data

The controller of personal data is the one who takes the decisions regarding the purpose and the means for the processing of the data. In the legal sense, there exists a controller whenever processing of data is taking place and it is the actual circumstances in each case that is considered. The controller is responsible for the processing being in accordance with the act and he or she can be held liable to damages if not so. This is the reason why only physical persons, legal entities and other institutions with legal capacity can be the controller of personal data.

A legal entity is most likely to be considered the controller, even if a physical person for organizational reasons and by internal regulations is appointed to have the responsibility. The question is whether such a person only has the right to search and use the personal data or if he has the right and possibility to change or correct personal data, which in that case could make him the controller.

Anyone who makes a database accessible to a third person, via a network or other on-line service, is therefore to be considered as a controller for that processing, but not for any further processing performed by the third person.

If two or more persons together have collected data, they are also responsible together for the storage and usage of the data. If anyone of them should use the data for any other purpose, they are all equally responsible and all liable for damages.

To be the controller of the personal data is to be the one in control and therefore also the one entitled to the ownership of the data. For a producing company this is a major argument in relation to the retailers. The producing company is the controller, meaning bearer of the legal responsibility and the risk-taker, and thereby entitled to the control and ownership of the customer database. Securing the content by complying to PUL, places all responsibility on the producing company, which in the same time acts as communication to enhance the perception of who is the rightful owner of the structure – the producing company.

5.2.7. Personal data assistant

Anyone who is processing data on behalf of the personal data controller is considered to be a personal data assistant. It is still the controller who is responsible and liable to damage, however the assistant treats the data.

An employee that processes data within the employment may not be considered controller. The employer is the controller and the employee merely an assistant.

If a company hires another company, legal entity or institution to process data, it will either be controller or assistant, depending on whether it is making the decisions on the purpose with the processing or not.

It may be possible to make a mother company controller, within a group of companies, even though each separate company is a legal entity. The processing of personal data could be organized so that the mother company takes all decisions regarding the purpose of the process and the other entities could then be considered assistants.

The producing company will in all circumstances be in control as regards to the personal data, even if the retailers or any other actors will be allowed to process data. All decisions regarding the purpose of the processing are taken by the producing company.
This is important as it communicates to the retailers that the producing company is the owner of the customer database.

5.2.8. Security

Anyone who processes data can do so only in accordance with instructions from the personal data controller. The controller is obliged to take technical and organizational measures to create a security level that ensures safe processing of personal data. This means in practice that anyone processing data is under a duty of not disclosing such personal data. If information is being disclosed in collision with such safety instructions, it is the controller who is responsible. Therefore it has been explicitly stated in the Personal Data Act that a written agreement is required between these two parties.

As regards the retailers, the contract can be in the form of a license agreement that contains the conditions necessary to fulfill legal requirements. The producing company can create the license so that the main issue is to fulfill the legal requirements regarding personal integrity and secrecy, and simultaneously make sure that the retailers accept the producing company as the owner to the customer database.
It is equally important to have written agreements with other actors, like external marketing firms and consulting companies, that are processing the data on the producing compnay's behalf.

5.2.9. Consent

The concept of *consent* is central and has vital interest when dealing with information and personal integrity. Consent shall be, as defined in the act,

voluntary;
specific;
preceded by information;
Unambiguous expression.

The prerequisites shall be interpreted so that there shall be no doubt concerning whether the registered person has been fully informed about what information is going to be processed and for what purpose and explicitly expresses that he accepts that his information is being processed this way. Such consent is considered a legal action and can be given by anyone with legal capacity. Because of the demand for preceding information, consent from each person must be given individually and for each process. A general consent cannot be accepted.

Other national laws have accepted the concept of opt out (silent consent) meaning that consent is the main rule until the registered person objects against it. This is not the case in Sweden. Neither is hypothetical consent accepted, meaning that even if one can be sure that the registered person would have consented if informed, it is not accepted to process the data.

In some cases the consent is demanded of the individual in order to get a service or to make a purchase. If it not is possible to refrain from giving ones consent, it can hardly be voluntarily and will not be an accepted consent.

It is not necessary to have consent in writing. However; in the eventuality of any future dispute, most likely the controller has the burden of proof and written documents could come in handy for evidence.

The registered always has the possibility to withdraw his consent. This influence on the registered's behalf has been limited so that already collected and processed data is not covered by a withdrawal. It is determined by a balance of interests when both the registered's interest of influence and possibility to change his mind as well the controller's interest and right to finish processing data that he has already collected with consent, has been taken into consideration.

The concepts of *consent* and giving *information* can not be stressed enough. The business value of a customer database is in all aspects related to how a company has communicated the purpose of the processing and received consent for the same.

The territorial scope

The Personal Data Act identifies the territorial scope as "for personal data controllers established in Sweden". The definition is unclear and not easily interpreted and the Data Inspection Board interpretation of the EC directive is working as a guideline. For establishment in a member state territory, one shall have an effective and actual establishment, through whatever legal form. It includes affiliates and subsidiaries. If the controller is established in Sweden as well as some other member state within the European Union, the Personal Data Act shall be applied for activities conducted in Sweden but for activities in the other state the situation is still uncertain.[8] Neither the EC directive nor Swedish preparatory work gives any further guidelines on where such activity shall be considered pursued.

The Personal Data Act also is applicable for the controller established only outside the European Union but using equipment for the processing in Sweden, unless it is done only for transfer of data between countries all of which are outside the European Union.

5.2.10. Requirements for processing data

The controller must always comply with general requirements, Personal Data Act, 9 §, when processing personal data.

The general requirements are not enough, but the processing must also be assignable to specific cases to be permitted. Such cases are stated in Personal Data Act, 10 §.

If the processing concerns sensitive information, for example personal code number or offences against the law, it must be specifically permitted in accordance with Personal Data Act, 13-22 §§.

If it involves transfer of data to a third country, outside the European Union, the processing must also be done according to Personal Data Act, 33-35 §§.

5.2.11. General requirements

The controller of personal data is responsible for the personal data under the following conditions:

- Only is processed if it is legal
When it is legal is as stated in the Personal Data Act.

- The data are processed correctly and in good practice
The expression "good practice" is a Swedish concept in the national legislation with no corresponding expression in the EC directive. How "good practice" shall be interpreted will be a question for the future when institutions like Data Inspection Board and different branches develop there own regulations.

- The data are processed for specific, explicit and justified purposes
The purpose, or purposes, must be decided in advance and not to vaguely expressed.

- The data are not processed inconsistent with the original purpose
The purpose may be changed only if the new purpose is not incompatible to the original purpose. This is maybe one of the most important regulations in the Personal Data Act and it

[8] See chapter "Operating on several markets"

leaves the controller with a great responsibility. The objection is to prohibit co-ordination and linking and matching of computer files. In situations when the personal data is to be distributed to someone else besides the controller, any new purpose must not be inconsistent with the original purpose. New consent from the registered is then not demanded.

- The processing is adequate and relevant for the original purpose
- No more personal data is processed then necessary for the original purpose
- The data are correct and, if necessary, up to date

The controller has to decide when these requirements shall be considered fulfilled.

- The data are rectified, blocked or erased if they are incorrect or incomplete for the original purpose

The controller shall spontaneously take all reasonable measures to comply with this requirement.

- The data are not maintained longer than necessary.

Personal data that can identify individuals must, as soon as it is no longer necessary, be made unidentifiable or hard deleted.

5.2.12. Permitted processing of personal data

The fundamental principal stated in Personal Data Act, 10 §, shows when processing of personal data is permitted. It is an exhaustive enumeration, and processing of personal data that is not mentioned in this section is prohibited.

Personal data may only be processed if the registered has consented or if it is necessary in order to do the following:

- To enable the performance of a contract with the registered person or to enable measures that the registered person has requested to be taken before a contract is entered into

It is a condition that *the registered himself* is a party to the contract or that it is the registered who has required certain measures to be taken before entering into a contract. It should be enough if the personal data controller provides information in advance that anyone who enters into a contract or requests certain measures to be taken for that purpose, may have his personal data processed, and that the potential registered thereafter takes such action, for consent to be given. An example of data processing that may be questionable is invoicing and customer data lists.

A contract between the personal data controller and a legal entity cannot justify processing of personal data on physical persons that are employed by the legal entity.

- For the controller to comply with a legal obligation

The definition of “legal obligation” is not yet clear, but it might be considered a situation where there exists a right to litigate and a right to have a verdict executed with the help of authorities, for example, enforcement service. (Kronofogdemyndigheten) Another example is the obligation to render account of social security costs for employees or labor law requirements on establishing an order of priority among employees when employments are to be terminated.

- To protect vital interests for the registered

Only personal data for the registered person is included, and that is even if he opposes this action. It is not possible to use this regulation as support for processing someone's personal data in order to protect vital interests for a third person.

- For a work task of public interest should be performed
Tasks of public interest includes the preparation of statistics, research work and opinion surveys. Registration of established sports organizations or commonly acknowledged rewards, such as the Nobel price, may also be of public interest.

- That the controller of personal data or a third party to whom the personal data is provided should be able to perform a work task in conjunction with the exercise of official authority.
The Swedish meaning of "official authority" is what is intended, for example when the police enforcement is conducting a preliminary investigation.

- That a purpose that concerns a legitimate interest of the controller of personal data or of such a third party to whom personal data is provided should be able to be satisfied, if this interest is of greater weight than the interest of the registered person in protection against violation of personal integrity.
This is a general clause and acts as a security valve. In some justified situations processing of data may be conducted even if not mentioned in the above stated situations. If a balancing of interests entitles the personal controller the right to process personal data, since his interest is greater, processing is permitted. However; in such a situation it is probably enough that the registered objects to it, for rendering him the greater interest. The processed data must then be made unidentifiable or hard deleted, since storage of personal data is considered to be a form of processing.

It is especially important when it comes to direct marketing, to consider the registrar's interest. The commercial interest must clearly overweigh if the processing shall be permitted.

5.2.13. Direct marketing

For the purpose of direct marketing, personal data may only be processed if the registered has not notified to the controller that he or she opposes such processing. The processing must also be permitted according to 10 §, Personal Data Act. If the processing includes transfer of data to a third country, outside the European Union, 33-35 §§ also must be complied with.

This means that the registered can by a written notification to the controller prohibit processing of his or her personal data for the purpose of direct marketing. The demand for a *written* notification implies that the opposition of the registered must be expressed in a text. Both in the form of a text on a paper or in an electronic form are accepted ways. Such a notification must be complied with even if the registered has left his consent previously. Only persons already registered can in practice be comprised by this regulation since there is no possibility for persons to prohibit processing of ones personal data in general and in advance. It would not be practical to make personal controllers organize notifications from persons that they might not be interested in and not having the intention of processing data of anyway.

All direct marketing activities are included, whether by ordinary mail, e-mail, phone or fax. Both commercial and non-profit purposes are included.

The practical meaning of this is that it must be possible for the registered to give his consent for several purposes but with the possibility to explicitly exclude direct marketing from the purposes of processing. This gives the registered the possibility to say no to direct marketing even if he has given his consent to processing of his data.

5.2.14. Prohibition of processing of sensitive data

Sensitive data are data that reveals race or ethnic origin, political and union affiliation, religious or philosophical beliefs, membership of a trade union, sexuality and state of health.

It is a fundamental principle that processing of such data is prohibited unless permitted according to 14-20 §§, Personal Data Act, for example if the registered has consented, 15 §, same act.

5.2.15 Personal Identity Number

According to the EC directive, each member state must, in national law, regulate the use of personal identity numbers. In Swedish national law that is done in 22 § Personal Data Act.

Data on personal identity numbers may only be processed when it is clearly justified for the purpose and the importance of a secure identification is clear. If there exists another noteworthy reason or the registered has consented, it may also be processed. If consent has not been given, the controller himself must balance the different interests.

There are two sides to the use of personal identity numbers. The advantage of secure identification is of importance for the protection of the individuals' legal rights. The fact that it is unique acts as a guarantee for the rule of law and a security for each and every person. In this sense the personal identity number is a protection for personal integrity. On the other hand, the vast use of such identification numbers has opened the door to misuse. The possibility of co-ordination of different registers increases the control of individuals and may thereby become a threat to personal integrity.

The personal identity numbers as such must not be considered a violation of integrity but any unnecessary use of personal identity numbers should be deemed as an infringement. All use of personal identity number shall be demanded only for approved and accepted reasons.

It is the Data Inspection Board's opinion, that there is no reason to process personal identity number when the purpose is to form a customer register in order to send information and customer benefits to the registered. Instead data on addresses and such could be updated by direct contact with the customer. When other numbers, for example customer number or member number may be used to identify each person, personal identity number should not be used.

Personal identity numbers shall at all times be avoided, if possible. Other impersonal identifications are recommended.

5.2.16 Information to the registered

Certain information shall be given to the registered *automatically*, by the controller, when it is collected, according to Personal data Act, 23 §. As a main rule, information shall be given in

advance to the actual processing, so that the registered is aware of what for and why he or she gives permission to the registration and processing of personal data. The information shall be given automatically, no matter in what way the data has been collected. For example if the registered himself has sent in his data to a company by e-mail, the data shall be considered collected and information about the processing shall automatically be given to the registered, by the controller. It is important that the registered is correctly informed. If the information given not is correct, it can lead to a fine or even imprisonment. The following information shall be given:

- The identity of the controller of the personal data. This means the name and address of the physical person or legal entity.
- The purpose of the processing of personal data.
- All information necessary for the registered to protect his or hers rights in connection with the processing. For example, who is the recipient of the data, and who has the right to the information and correction.

There is no obligation for the controller to give information to the registered party more than once concerning the processed personal data all at the same time, as long as the purpose still is the same or is not inconsistent to the stated purpose. If the data is transferred to someone else for processing, further information about this is needed only if this information not was given in the beginning. It is the responsibility of the controller that the information reaches the registered. If the purpose is to collect new data on the registered continuously, each new collection of data should probably be informed. Whether it is directly to the registered or to an intermediary, it is the responsibility of the controller that the information reaches the registered. Of course the information must be in a language the registered understands but there is no demand for written information.

When personal data is processed in connection with Internet and electronic billboards or any other electronic services, it is suitable to have all such information on the sign-on screen. If the information has been collected from some other source than the registered himself, the information is preferably sent to the registered by mail.

Some information shall be given to the registered after a specific *request*. Each person has the right to once a year receive a record, free of charge and in writing, on what is being processed. This right gives the individual an opportunity to control whether he or she is registered, if the data is correct and if not have it corrected.

The following information shall be given on request:

Which information concerning the registered that is being processed
Where this information has been collected
The purpose of the processing
To which recipients or categories of recipients the information has been disclosed. (General information can be accepted, such as “recipients are companies within the same group of companies”.)

Information shall be given under two different circumstances. Once automatically during the first actual collection of personal data. Secondly, the registered has the right to request information once a year.

5.2.17 Correction

The registered has a right to request for his personal data to be corrected by correction, blocking or deleting. The controller is obliged to inform any third person that has received the data, about any correction.

The law does not regulate whether correction, blocking or deleting shall be used when correcting data. That is up to the controller to decide. In case of correction, false data may be replaced with correct data, and if that is not possible, blocking or deleting shall be used. Correction shall be performed *as soon as possible* after the request from the registered.

Deleting of data must be permanent destruction and not done in a way that it is possible to recreate the data.

> It is important to have a procedure for how to correct and destruct the personal data as it otherwise may not only cause legal problems, but also customer bad will. To delete data means that it shall be ”hard deleted” in the meaning that it shall be impossible to recreate.

5.2.18 Transfer to a third country

Transfer of personal data to a third country is only permitted, according to the main rule in the EC Directive, if the third country has an adequate level of protection for personal data. Certain rules for determining this level of protection has been drawn up and the commission has the power to make the decision.

However, a personal data controller can, according to the EC Directive, transfer data to a third country without this high level of protection for personal data, if he with certainty can guarantee that adequate protection is provided by for example a contract that regulates the transfer.

The data may also be transferred to a third country if the registered has given his consent or if it is necessary in order to fulfill a contract between the registered and the controller.

It is also permitted to transfer personal data to be processed in a third country that has acceded to the Council of Europe Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data.

5.2.19. Internet

When personal data is being made available on a global network, for example on a website on Internet, it can be reached by anyone, most certainly also by third countries without an adequate level of protection of personal data. This makes personal data available in a way that is prohibited by the EC Directive.

Such global spreading of personal data is only permitted if the registered has consented. Neither the Swedish law, Personal Data Act, nor the EC Directive permits such processing of personal data Except for the situation with consent from the registered, it is not possible to generally permit processing of personal data and then make it available on Internet or global networks.

The meaning of the prohibition of publishing personal data without consent on the Internet, is to emphasize the fact that all personal data shall be handled confidentially. All data on the Internet is accessible world wide with no consideration of the different country's level of protection for personal integrity. This is not acceptable from a legal point of view and not recommended due to company good will.

5.2.20. Notification duty

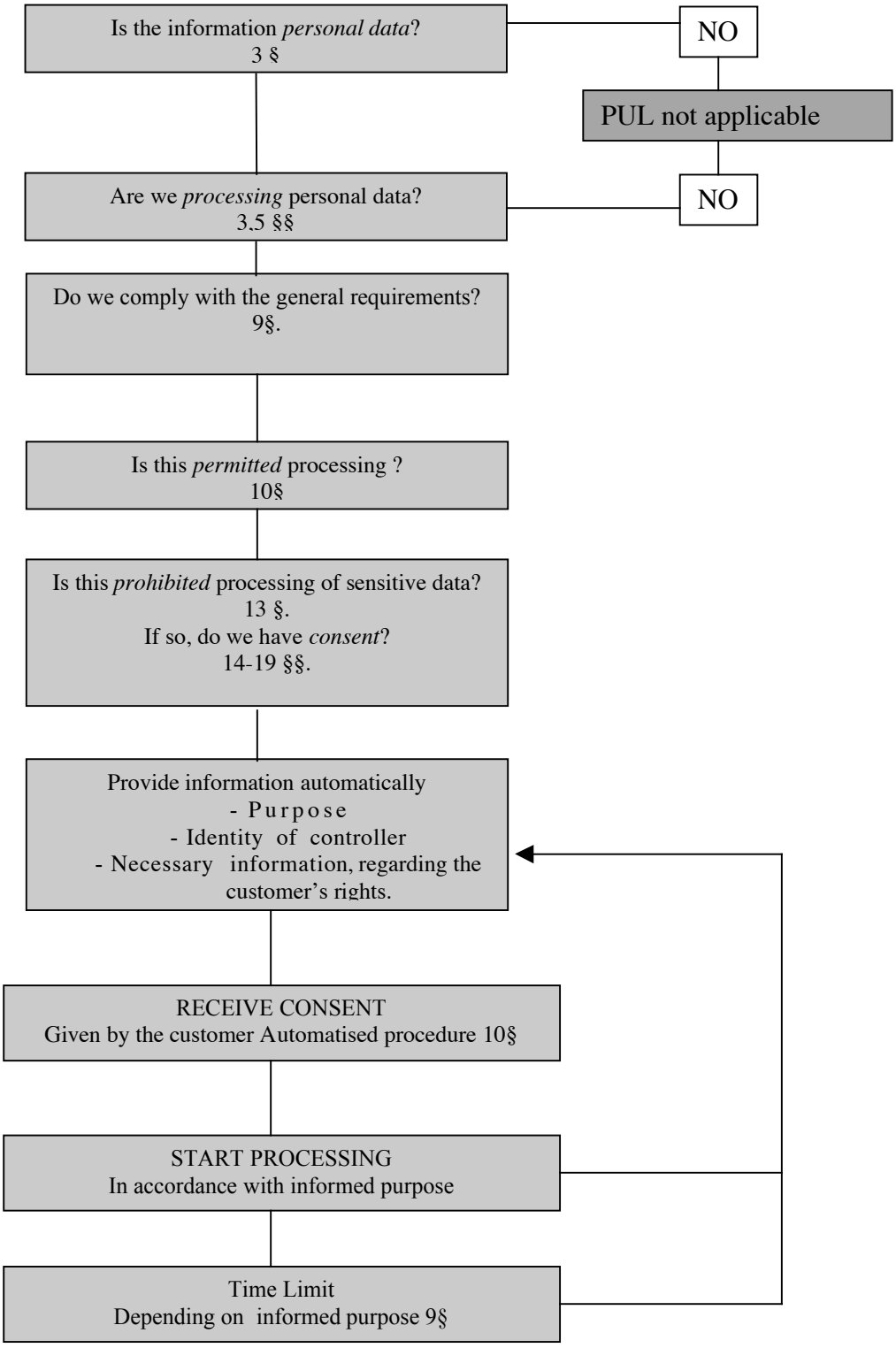
Anyone processing personal data has in principle a duty to notify the supervisory authority, the Data Inspection Board, before processing. One can be exempted from this notification duty by appointing a personal data representative who supervises the processing of personal data, so that it is performed legally, correct and in accordance with good practice. It is possible to appoint an employee as representative as long as his or hers position is independent from the employer.

The representative shall call attention to any deficiency and imperfection and if necessary notify the supervisory authority. There shall also be kept a record on the processing that unless the representative was appointed, should have been notified to the supervisory authority.

This is a ”remain” from the Data Act, preceding the Personal Data Act, according to which all companies processing personal data had to register to the Data Inspection Board. Today companies must appoint a personal data representative, that ensures that all data is processed in accordance with legal requirements and *otherwise* will rapport to the Data Inspection Board.

This flowchart can be seen as a summary of which steps a company must take when processing personal data. Following these steps may be the beginning of handling personal data in a correct manner.

PUL-Checklist



5.2.21. Operating on several markets

The Swedish Personal Data Act is based on an EC directive. However, the different member states have the freedom to choose how to implement the directive into their national legislation. The fact that the directive has been interpreted differently throughout Europe has lead to the result that the national legislation differs between member states, although the legislation is based on the same directive. The directive is rather new and, in addition to this, in some parts difficult to interpret. This has been commented by the Swedish government in the preparatory works[9], and has been discussed in the committee that was created in accordance with article 31 in the directive. In the near future the Court of the European Union will create a unified solution. Until this is achieved it is therefore important to, with the directive in mind, have knowledge of and comply with the different member states legislation[10]. This is stated in article four in the directive:

National law applicable

1. Each member state shall apply the national provisions it adopts pursuant to this directive to the processing of personal data where:

a. The processing is carried out in the context of the activities of an establishment of the controller on the territory of the member state; when the same controller is established on the territory of several member states: he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

5.2.22. Opt in – Opt out

The choice between the different concepts *opt in* and *opt out* is today probably the major difference between the member states ways of implementing the new legislation on personal integrity. Some European countries, like Sweden, have adopted the concept of opt in which means that you may only use personal data for marketing and other purposes if the individual involved has intentionally given his consent before hand. In countries where opt out have been chosen, information is being collected for marketing and other purposes and the individual has the opportunity to stop the processing of his personal data afterwards. If that option is not exercised then the company may use that information for those purposes.[11]

This can be illustrated by the following example:

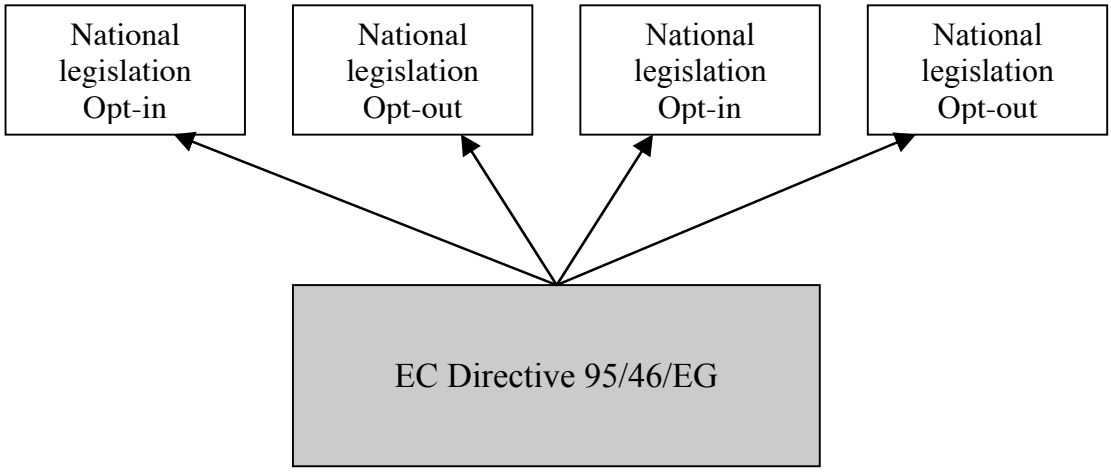
> A company in the UK uses an e-mail marketing list and on that list is the e-mail address of an individual in Sweden. The company in the UK may decide to market that person, as according to the UK personal data act, the list should only contain the details of those who not (yet) have chosen to opt out of having their e-mail addresses used for marketing purposes. The Swedish recipient of the marketing would no doubt consider that the company sending the marketing e-mail may have committed a criminal offence, since sending unsolicited marketing communications in Sweden is an offence. To be able to send the marketing to the Swedish individual the company must be sure that the individual has been informed and given his consent of the marketing when submitting his personal data, as this consent is required by the Swedish Personal Data Act.

[9] Proposition PUL (1997/98:44), SOU (1997:39)
[10] Contact with Anders wiklund and Elisabeth Wallin, Datainspektionen
[11] Contact with David Clancy, Strategic Policy Officer, Information Commissioner's Office, UK

This complies with the Swedish official investigation[12], saying that if the personal data controller is established in several member states the Swedish legislation shall be applied on the personal data processing performed in Sweden, but not in the other member states. Therefore one needs to comply with each member state's legislation.

The difference between opt in and opt out can be summarized by saying that it is a question of whom shall be the active party. Opt in means that the company must act to get an intentional consent from the individual, why opt out means that the individuals consent is default and that he must take action to withdraw it. To be on the safe side regarding this issue it is best to always follow the opt in route.

Opt-in:
Consent → Processing
Opt-out:
(silent consent) Processing → withdrawal of consent



When operating on several markets our recommendation is that always have an opt-in routine as this is accepted in all countries effected by the directive.

5.3 Other regulations

Even if all requirements regarding PUL are fulfilled, a company must be aware of the fact that other activities related to personal data may be regulated by other acts. Activities such as marketing, games and lotteries can for example actualize an intervention from the authorities according to different applicable laws. To comply with PUL is however the most essential

[12] SOU (1997:39)

task for a company involved in e-CRM activities, because most actions that a company would like to perform is legal as long as the actions are built on consent.

6. Securing the structure

The section will describe what kind of regulations a company may use to communicate the fact that it considers its customer database to be a legally protected object, as well as what actions the company can take to enhance the perception of the customer data and database as property. The section will start out by describing the meaning of copyright, and how the protection of the database structure can be derived to this legal instrument. The section will continue by describing and explaining the database directive and investigate how this regulation can be used to secure ownership to the customer database. The section also contains an overlook of the Swedish act on trade secrets and an explanation of how this regulation can be used together with a licensing structure.

6.1. Legal protection of structure and content

6.1.1 Copyright

The right for artists and authors to be acknowledged for their intellectual achievements has been a fundamental base during history for the cultural and economic development of nations. It has been considered essential that creative achievements and its achievers shall have the possibility to harvest the winnings of their work and prohibit others from copying and using it, and in this way encourage inventors and others to continue to contribute to society.

The rights that derive from having legal protection for an achievement can be divided in two different sub rights: The economic right and the ideal right. Where the economic rights give the right holder the exclusive right to restrict others from commercializing the achievement such as to transfer, license or use it, the ideal rights are aimed at letting the achiever enjoy the recognition from the society for his work, and prohibit certain offending usage of it.

A basic principle for that intellectual work shall enjoy protection has been, and is still, that the intellectual achievement is new and unique and that it reaches a certain level of creativity. This principle has been essential, not only to create a system that can exist without being to unsure, but also to be able to decide which kinds of achievements that are worthy of protection. In recent years there has been a debate though whether certain intellectual property should have the right to protection without reaching a certain level of creativity and without being unique.

The basic principle behind this debate is that in many situations there is needed a great deal of investments in time and money to create an asset that although it may not be unique or creative has earned the right to protection due to the investment. So the economic protection has in certain situations shifted from protecting the originators right to earn the financial winnings from the achievement, to protect an investment that has been made to create the achievement.

The area in which this is most distinct is the protection of great collections of data such as in databases. Databases of different kind are often the result of a great deal of investments in time and money, and can also be of great value for the originator. As a result of a common understanding within the EU that databases did not enjoy an acceptable level of legal protection in all EU countries, the EU founded a directive (96/9/EG) aiming to insure that the protection was similar and acceptable throughout the union. In Sweden the directive resulted

in a change in the Swedish copyright act that came in force the first of January 1998. This directive will be handled under section ???.

6.1.2. The Database directive

A database according to the Database directive[13] is defined as follows:

" Whereas the term "database should be understood to include literary, artistic, musical or other collections of works or collections of other material such as texts, sounds, images, numbers, facts and data; whereas it should cover collections of independent works, data or other materials which are systematically or methodically arranged and can be individually accessed; whereas this means that a recording of an audiovisual, cinematographic, literary or musical work as such does not fall within the scope o this directive."

A systematic collection of data can consist of phone numbers, stock rates, exchange rates, time tables, and so on. It can also be a collection of short novels, poems or photographies.. The collection can be attached to different technological media such as written on paper, or saved on a hard drive or disquette.

6.1.3. Copyright protection of databases

Already as early as 1919, in the preambles to the Swedish copyright act, it was stated that a systematic collection of data could be considered as a work of art and therefore be copyright protected under article 1 in the Swedish copyright act.[14] For a work to be considered as a work of art though it must have some originality and independence and therefore must be the result of some sort of intellectual achievement of some quality, or in other words the result of a planning, collecting, evaluating and editing activity.

The basic principle regarding copyright protection for systematic collections of data is that the same criteria shall be applied as for other kind of works. This means that for a customer database with ordinary personal data to enjoy copyright protection there must be something unique and creative about the way it is organized or structured. To achieve this can be not only difficult but would also create an unnecessary amount of work. This essay will therefore not further handle the possibilities of a copyright protection.

The customer database can of course also be protected by keeping it secret and have an internal usage policy for the employees, but there may be situations when an external actor or companies within a consortium may come in contact with customer data why being aware of the legal protection is essential. A customer database falls within the scope of the Trade secret act that will be handled below.

6.1.4. Sui generis, right of its own

The EC directive was developed to insure a high protective level for databases in all member countries. This should be achieved by the directive imposed on the member states to create a legal protection for databases that should exist side by side with the copyright, protecting databases that do not reach up to a certain level of uniqueness and creativity. This so called sui generis protection should according to the directive be a complement to the rules on copyright, which means that there will exist databases that are subject to both copyright and

[13] 96/9EG, Preamble art.17
[14] SFS 1960:729

sui generis protection. Where the copyright protects the intellectual achievement, the sui generis protects the investment that has been performed to create the database.

The subject for protection is, according to the directive[15], databases that have come into existence by a substantial investment, stating:

”Member states shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.”

6.1.5. The sui generis property right holder

In the preamble to the directive it is stated that the exclusive right for the producer shall ensure protection of any investment in obtaining, verifying or presenting the content and that the investment can consist of either the deployment of financial resources and/or the expending of time, effort and energy. What a substantial investment consists of is not further defined in the directive, but has been commented in the doctrine.[16] It is the producer’s responsibility to show that such an investment has been made.[17] How this can be done is not stated in the directive, thus ordinary rules of proof will be applicable. It is therefore important to create clear and precise contracts, so that it is easy to prove who the investor is.

The directive[18] identifies the investor as the producer and the legal rights owner to the database stating:

” Whereas the objective of the sui generis right is to give the maker of a database the option of preventing the unauthorized extraction and/or re-utilization of all or a substantial part of the contents of that database; whereas this exclude subcontractors in particular from the definition of maker;”

In cases where a company itself creates a customer database the ownership will belong to the company due to the fact that the company is the investor, paying salaries and devoting their employees working time to the project. This is not the case with copyright, (computer software excepted) where the copyright stays with the employee if nothing else is agreed. The article is perhaps even more important as it means that a company can contract, for example a consultant, to create a customer database and still become the legal property right holder even if the company is just contributing financially by paying for the consultants work. This is not the case regarding for example copyright. A consultant that develops a software program for a contractor remain the copyright property holder, if nothing else is agreed upon, even if the contractor is the party taking financial risks.

[15] 96/9/EEG, Art. 7(1)
[16] Jensen, N ordiskt Immateriellt Rättsskydd (NIR) 1999 s. 64 ff
[17] 96/9/EEG, Preamble, Art. 54
[18] 96/9EEG, Preamble, Art. 41

6.1.6. What the right encompass

The sui generis protection means that the maker of a database can prevent others of extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the content of that database.[19] Extraction and re-utilization is defined in the directive:[20]

" *"extraction" shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form"*

" "re-utilization" shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission."

This means that the protection does not protect the specific data collected in the database. It is only the database as such that is protected, or in other words, the whole or a substantial part of the database. This means that what can be protected by the Database directive is not the content but the structure. However this rule is complemented by another article[21] stating:

" The repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflicts with a normal exploitation of that database or which unreasonable prejudice the legitimate interests of the maker of the database shall not be permitted."

This article aims at protecting the investment behind the database, where even an insubstantial part of a database that is used incorrectly can harm the producer financially.

The directive does not inflict on the database owner's right of disposal. A database as such shall be seen as property, which means that ordinary property laws are applicable. This means that a database can be the subject of different kinds of transactions. It can for example be purchased or out licensed. In the agreements following such a transaction it is of utter importance, that the true subject of the transaction is defined. For example a license agreement must define what is being licensed, to further stress the fact that the licensee is handling the licensors property. How a database user license agreement can be written will be discussed and exampled further on in this essay.

6.1.7. Time of protection

According to the directive a database is protected 15 years from the time it was finished or was first available to the public.[22] These regulations are complemented by another stipulation stating that a new and essential investment in an already existing database can have the effect that the database is seen as a new database and therefore resets the timeframe, creating a new 15-year protection.[23] The burden of proof that such an investment has been made lies in this case (i.e. in proving that an initial investment has been made) with the investor. As such an

[19] a.a. Art. 7(1)
[20] a.a. Art. 7(2a,b)
[21] a.a. Art. 7(5)
[22] a.a. Art. 10.1 and 10.2
[23] a.a. Art. 10.3

investment can be considered a thorough editing and overlook of the database, even if nothing new is added.

The difficulty with the database directive regarding customer databases is that the directive's goal is to protect databases that are finished in the sense that they are not regularly worked with, and therefore static in there existence. A customer database however, to be of any value must be constantly renewed and worked with. This is why it can be difficult to put an exact date on when the investment was enough to be considered essential, and therefore worthy of the sui generis protection and also to decide when the CDB can be considered to have been the subject of a such essential investment regarding editing so that it can be considered a new database.

If the producing company collects data from the retailers and store this data together with previously collected personal data that is supervised by the producing company, this supports the fact that *a new database is created*. This new CDB is protected from this point in time and 15 years ahead. By doing regular updates and overlooks of the CDB, the producing company can make sure that the CDB is protected indefinitely. The condition is that the updates are considered essential.

6.2. Swedish act on trade secrets

Most companies have information spread within their business that they want to keep secret from the public and other commercial actors in the market. At the same time it can be important to share information with business partners and companies within a consortia and this explains why the legal protection of the information must be clear and precise.

The technical development during the last decades has made it possible to easily and effectively collect, save and transfer customer data. Thousands of existing or potential customers can be stored and sorted after different criteria. The average consumer is every day exposed to hundreds of different commercial messages. For a company, to be able to stand out from this mass marketing, it takes a lot of money and time, and added to this you can never be sure that your marketing reaches the right group of consumers.

These simple facts can begin to show how cost effective it will be in the future to attract only the consumers that are potential customers, and above this to make them feel chosen and special to not only buy your product once, but also insure customer satisfaction and to make them be loyal to the brand. This management of customers, together with creating ways of transforming customer relations into structural capital will give companies a competitive advantage in relation to other actors in the line of business. This also means that a company's customer relations in fact is one of the most valuable trade secrets they own, and why considering them as such is vital not only for creating a legal protection, but also as a mean of communicating this to employees and business partners.

6.2.1. The object according to the trade secret act

The legal definition of a trade secret is wide. The act on trade secret states three objective criteria that determine whether something shall be considered a trade secret. These criteria are:

1. It shall be information about business or production in a commercial context.
2. The company shall keep the information secret.
3. A disclosure of the information shall aim to be of damage for the company from a competitive point of view.

To be able to claim responsibility for an attack on a trade secret two more criteria must fulfilled. These criteria are:

1. The attack must be unauthorized.
2. It must have been done on purpose or in some cases by negligence.

The information describes the object of the protection. For the information to be worthy of protection there is no demand for it to have any kind of originality or patentability. This makes it important for a company to by itself define what information that is of importance for the business and therefore must be protected as a trade secret. This perception must also be communicated to parties that will come in contact with the trade secret, thus explaining why a trade secret protection must be complemented by a contractual structure.

Besides the protection given to the database' structure by the Database directive, a company can in addition use the act on trade secret as a communicative tool to establish an understanding of the fact that the customer relations, as being the content of the database, are legally protected. Breach against company guidelines regarding this would not be simply a breach against contract but also against a legal act.

The technical possibilities to create an effective customer database today, combined with aimed marketing offers, will be the most powerful tools, not only to reach and attract the consumers that really are interested in becoming the companies customers, but also to make them loyal and satisfied customers. This makes it important to consider customer data as valuable trade secrets.

7. Interaction with other intangible assets

This section will define a trademark, and why it is important to consider the same when discussing a customer database and processing of personal data. The section will give an overview of the legal concerns regarding trademarks, as well as a more strategic analysis.

A company has better opportunities to be successful if they are aware of how it can use its different intangible assets to interact with each other and thereby create different business strategies. The trademark is what attracts customers and therefore creates the customer relations and the customer database. It is the investment in the trademark that is the basis for the customer database why how the data is being collected from a practical point of view is of no importance from an ownership point of view. To be able to govern a customer database and give it a value the trademark strategy therefore must be structured to interact with the customer relation and customer database strategy. This is why this section if of importance to understand the whole picture.

7.1. Trademark protection

Trademark protection is an intellectual property right that protects *distinctive and characteristic marks*. According to Swedish law, Varumärkeslagen (1960:644) VML, this protection may arise in two different ways, either by registration or by being established in the market. It has been considered important to not only have a system of registration, to stop unwanted market encroachments, such as for example when competitors register trademarks simply to hold back another competitor. One requirement for registration is that the mark has the ability to distinguish between trademarks, and that is for many not obtained until after establishing on the market. Therefore it has been considered important to create a protection that also covers trademarks that are not (yet) registered, but still well known on the market. [24]

The conditions for registration of trademarks are that the mark can be reproduced graphically, has an ability to be distinguish between trademarks and that it is not confusing to another already existing trademark. If these conditions are fulfilled and the trademark is registered, the holder of the right must make use of the mark within a time period of five years. The registration lasts for ten years and may be renewed indefinitely.

The trademark is the link between the company and its products and the customer, and that link is what is to be protected, not the customer as such. Anyone is permitted to try to attract someone else's customer, as long as this is done by fair means. To disrespect other's trademark is to harm that link since it could be confusing to the customer. The customer relies on the fact that a certain product originates from a certain producer, and thereby expects the quality that the specific trademark guarantees. The holder of the trademark right often puts a lot of effort and invests enormous amounts of money into the trust that building a strong brand constitutes. This trust between customer and trademark holder can easily be ruined if the trademark is not protected properly, against misuse. The exclusive trademark right gives the holder the right to prohibit others from using his trademark or confusing marks except when permitted by a license agreement.

It is the link between the customer and the company and its product that is protected by trademark law.
The trademark represents a value and a quality and the law is designed to protect the owner's investments in the branding, in order for consumers as a weaker party not to be confused of a product's origin.

They have a recognizable quality that can be tempting for disloyal behavior and therefore constitutes a serious risk for damage for the trademark holder. Misuse of the trademark can cause dilution. In a famous example from 1898 someone used the trademark KODAK for selling bicycles, and there was clearly no risk for confusion since the goods were quite different. Still KODAK managed to stop the use of its trademark because of the risk for dilution. The KODAK Doctrine was created, based on this case, and it defended the trademark's value and commercial function without taking the similarity between goods into account. Also the Swedish VML added in 1993, because of its adjustments according to the

[24] Koktvedgaard, M; s 310f

EC directive, a clause that protects well-known trademarks. [25] This new regulation also covers the so called Rat Poison Rule (Råttgiftsregeln) stating that certain trademarks, such as trademarks for perfume, may be extra sensitive to the similar trademark use of others, for example for rat poison.

7.1.1. Community Trademark

Trademark protection is the first legal discipline in the area of intellectual property to be regulated in a unified European order. Such a system of registration is considered necessary, if the European Union shall have a common trademark protection. A directive and a regulation have been created and constitute the protection that directly covers the European Union.[26]

Therefore, as of 1996, it is possible to file an application for a community trademark, to secure unitary trademark protection and to have legal consequences in all member states within the European Union. By requiring one application the trademark owner gets protection throughout the EU by using the trademark in only one country and there is no demand for designation of countries within the union. Previously, to obtain a protection covering the entire European Union, the trademark owner had to file applications in each separate country, according to different trademark laws and in different languages. Today it is one administrative procedure by one administrative body, the Office for Harmonization of Internal Market (OHIM)[27] in Alicante, Spain, and the applicant chooses from one of five official languages to be used for opposition revocation or invalidity proceedings. OHIM has the authority to refuse an application on absolute grounds, such as lack of distinctiveness, or if the trademark is misleading, or if the owner of an older trademark registration files opposition against it. If there exists obstacles for registration in one country, the trademark cannot be registered as a European trademark. The term of validity of a community trademark is ten years and it may be renewed indefinitely.

This community trademark does not replace the respective laws of the member states in this area nor does it eliminate the national trademarks, but coexists with them. If the community trademark application is refused, withdrawn, or deemed to be withdrawn, or ceases to have effect it may be converted into one or more national trademark applications. The national trademark application resulting from the conversion shall have the date of filing or the date of priority of that application.

7.1.2. Treaties and international system

Several different conventions and treaties exists in this area, such as the WTO agreement TRIPs [28] The agreement defines what types of signs must be eligible for protection as trademarks, what the minimum rights for the owners must be and what marks have become well-known in a particular country and therefore enjoy additional protection.[29]

[25] VML, 6 §, section 2; which replaced the old Kodak protection.
[26] Directive 89/104/EEG, Regulation no EEG 40/94.
[27] The CMTO = Community Trade Mark Office = OHIM = Office of Harmonization of Interior Market
[28] TRIPs; trade-related aspects of intellectual property rights
[29] www.wipo.org

The Madrid Agreement is an international system and even more important is the Protocol that belongs to the agreement. An international registration according to the protocol, is based on a national application, and administrated by The World Intellectual Property Organization (WIPO).[30] It is an international organization and one of the 16 specialized agencies of the United Nations. It administers 23 international treaties dealing with different aspects of intellectual property protection. The organization counts 177 nations as member states.[31]

7.1.3. Domain Name and Trademark

The existence of Internet creates a new set of problems for the legal framework to handle. The usage of domain names, and their concomitant conflict with trademarks, are still problems have yet to reach a unified solution. The legal regulations regarding trademarks, both nationally and internationally, gives the holder of the right an exclusive right to use the trademarks and any rising conflicts should be solved in accordance with already established principles. The problems occur when someone registers a domain name that is exactly as or confusing to someone else's trademark. The Internet is global and traditional trademark legislation is applicable mainly on a limited territory. The legislation of the country where the infringement takes place shall be applied but on the Internet it is not clear whether the sending country or receiving country is the infringing country.

The registration of domain names that are in conflict with trademarks can be done in good faith but there is also the case of cyber squatting – domain name piracy. Unfair competition and trademark laws have successfully been used against such behavior.

Commercial actors must have the right to their trademarks as domain names. The fact that trademarks as domain names are registered at all actually gives a double protection, which, one can argue, should not really be necessary. (See also section "Trademark preempt domain names")

The owner of a trademark is the holder of the trademark rights as well as the only possible owner of the domain name. Internet websites using the brand to attract customer, may be organized by retailers but customer data and the established relation is a direct correlation to the trademark and its inherent values.

7.1.4. Parallel import and trademarks

The principle of exhaustion of right is important when it comes to the issue of parallel import. Parallel import means that someone else but the holder of the right, brings the product into the European Union after it first has been released *outside with permission* from the holder of the right, by importing it from this third country outside the European Union and EES. A retailer in EU may have obtained a permission to market and sell products from his principal and underwent the necessary investments to establish the trademark on the local market and created an organization with warehouses and services. A parallel importer often has the possibility to sell the same products at a lower price since he has not had the costs for advertising and maybe does not provide service and so on. Although this undermines the authorized retailer's organization, the main ruling has been that he cannot stop this parallel import. It is the holder of the right, the principal, that has equipped the product with his trademark and it is not confusing to the customer who is not misled. It is in fact the product

[30] Koktvedgaard/Levin, "Lärobok i Immaterialrätt", s 304f
[31] www.wipo.org

that the customer can expect because of the trademark. It has been considered too much power to give to the local trademark holder to inhibit competition if it should be possible for him to stop such import because of his exclusive right to the trademark.

If the products have been changed or deteriorated the trademark holder would have a reason to stop the use of his trademark. The sale of substandard products may of course bring harm to a trademark. This situation often occurs with goods with a longer life cycle, such as cars. It is very common with sales of extensively renovated cars that no longer include any original parts. This must naturally be possible for the rightful owner of the trademark to stop, which is made possible according to both VML and the directive.[32]

According to a major principle in the EC Treaty,[33] the treaty shall not affect national property right. National regulations may however not constitute means for arbitrary discrimination or disguised limitation of trade between the member states. Non-discriminatory national legislation on protection for intellectual property may be in conflict with the main principle of free movement of goods within the common market. Therefore the EC, on the basis of the EC Treaty article 308 that can be used to take special measures in order to fulfill a main principle of the EC Treaty, has started to harmonize some parts of intellectual property right legislations between the member states. An international legal order is also being developed, as there are many conventions on this area today.

The Swedish Varumärkeslagen (1960:644) VML contains a rule of exhaustion of right[34], based on the EC directive.[35] It states that the owner has his exclusive right exhausted when the product is released and marketed on the EES territory. This means that parallel import then is permitted to the region. However, the question on *how the trademark* then may be used, when it comes to advertising and commercial activities, is still not satisfactory answered. The EC court has established that importers on this so called "grey market" have the right to use the trademark as long as they do not cause *serious damage* to the trademark. Swedish practice has not been so generous but talks rather about that the importer can use the trademark *most restrictive*. A parallel importer must be loyal to the trademark in his use and never use it as his own or take advantage of its good reputation.[36]

Because of the desire for increased competition, the exhaustion of trademark right first was made global. Now the situation seems to have changed. The EC court has given their answer to the problem in the Silhouette-case where it was established that article 7.2 in the trademark directive implies that only *regional* exhaustion arises when products are marketed in the European Union, not globally. [37] Competition authorities as well as consumer associations have been critical and argued that such limitation of the exhaustion of rights will lead to an increase of prices if cheaper parallel imported goods are stopped.[38]

Competition law and the all-embracing objective of the European Union, free movement of goods, may seem to friendly to un-authorized retailers. Once again the importance of the trademark and trademark rights must be stressed, since this is a possible way of controlling such retailers.

[32] 4a § 2 st, VML and article 7.2 89/104/EEC
[33] EC Treaty, article 295
[34] 4a §, VML
[35] article 7.1, 89/104/EEC
[36] Koktvedgaard, M; s 337
[37] C-355/96; 16 July 1998
[38] Koktvedgaard, M; s 343

7.1.5. Trademarks preempt Domain Names

After years of building a strong brand, advertising and promoting the quality of ones products, one of the most important assets for a company may turn out to be – their name.

In today's economy many companies are conducting business over the Internet, since the use of this media has increased and is widely spread today. They use their famous name to market themselves and to attract customers and one important step is to register domain names. Sometimes companies and famous persons find that their name have already been registered by someone else. A so-called cybersquatter register domain names, with the purpose of receiving a ransom payment from the trademark owner, to buy the domain name back. In the US, who in many ways is a legal precursor in this area, traditional trademark law did not make such action illegal. [39] To sue for trademark infringement a consumer had to be confused as to the source of the product and most cybersquatters did not sell products at all or sold possibly different products. *The Federal Dilution Act of 1995* was therefore enacted, to protect famous trademarks from dilution and to stop those who attempt to benefit from what others have invested time and money, in developing a trademark. The owner of a valuable right such as a trademark shall have its property protected from being eroded, blurred, tarnished or diluted. The act does not require consumer confusion as a prerequisite to there being a violation.

Only famous trademarks are protected by this act. The misuse must be commercial to avoid free speech concerns and the trademark has to be diluted as a result of this. So far the interpretation of dilution has been widely interpreted to mean that any lessening of the capacity of a famous trademark to identify and distinguish is considered a dilution, regardless of the connection between the right holder and the infringer concerning competition and so on.

In 1999, *the Anticybersquatting Consumer Protection Act* was enacted. That a famous trademark is registered as a domain name in "bad faith" is a requisite in order to deal with the situations when a cybersquatter simply sits on the domain name.

The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for regulating the issuance of the domain names on the Internet, due to a contract with the United States government. ICANN approves registrars of domain name. They have also approved an arbitration procedure for challenging cybersquatting, *the Uniform Dispute Policy* (UDRP) that requires all ICANN-approved registrars of domain names to agree to use the dispute resolution policy as part of their accreditation. Any disputes are than heard by an arbitration panel, approved by ICANN.

7.2. Trademark connection to customer data

An important issue is a retailer's use of a trademark, belonging to his principal. The retailer often does the actual marketing and establishes the trademark on his local market and he may therefore argue that he has some right to the trademark as well. However, if nothing else is regulated contractually, the right to a trademark follows the product it represents, and by that it will belong to the principal. This may seem obvious, but it is still extremely important to bear in mind. Especially when a company is established on a new market as the result of a local retailer's actions, no matter the amount in time and money that the retailer has invested, the trademark always belongs to the principal. To understand this, it is of importance to know the difference between the tangible products and the intellectual property rights that are

[39] Cheeseman, s 339ff

attached to the tangible. A customer that buys a product has the right to that very tangible copy of the product, no matter if it is a car or a book. This means that the customer has the right to sell it, use it or even destroy it if he seems fit. The intellectual property rights attached to the product, such as copyright for a book and patents, trademark, licenses a.s.o for a car will however still remain with the principal. The same situation arises when a local retailer sells products under a retailer license. The retailer has the right to sell the cars, using the trademark in accordance with the principal's guidelines but the ownership and control of the trademark still remains with the principal. As we state that the customer relation and the customer data is the result of the investment in the trademark, which at all times remain with the principal, the customer data should belong to the principal at all times as well. The retailer can only be seen as a middleman, that mediates the contact between the principal and the customer. If the retailer is taken away, the relation between the principal and the customer still remains as a result of the trademark and the customer relation objectified in the customer database.

7.2.1. Old and new customer data

The customer data that could be of interest for the customer database can be divided into two groups. Firstly the data the company already controls. This includes data that are already in the database as well as data that are to be collected by the company and the business partners after a contractual structure has been established.

The second group consists of the customer data that has been collected by retailers and other business partners, as a result of transactions being performed with products sold due to the principal's trademark. To be able to gain control over this data, the principal must convince the other parties that the data belongs to the owner of the trademark, as an effect of the principal's investment in the trademark. These investments are executed in the first place to make the trademark well known, and therefore constitutes a prerequisite for that the customer data could be collected at all This, together with the database directive described above, stating that the owner to a database is the main investor, are circumstances that points only in one direction - the principal is entitled to claim ownership to the customer data not yet in control.

The trademark is the obvious reason why customer data can be collected and stored. How the customer data practically is collected is of no importance. All customer data, old and new, shall therefore be the property of the trademark holder.

8. The license construction

As it may be valuable from a business perspective to allow business partners to use a company's customer database the next section will start to describe which kinds of considerations and strategic choices a company must take into account when deciding how a licensing strategy should be built. As this is a complex area that needs to be carefully governed, the section will only describe the different strategic choices from a broad perspective. A detailed analysis must be performed before entering into any kind of license agreement.

To create a license construction, as well as the company's entire contractual structure for different relations, is to implement and operational the results or effects of the interpretation that has been performed.

Intangible assets may be valuable not only for usage within the business, but also as a way of creating income or new business structures by out licensing. The main conception of licensing is that it can only be used as a way of giving permission to someone else to produce or exploit a certain technology. However, the license construction can be used in numerous ways.

Licensing in the past has primarily been used for licensing technology when companies wish to conquer new markets and set up new retailer relations. It can also be used for different reasons such as creating business relations and strategic alliances, transmission of knowledge, to strengthen the company's competitive position, to minimize the risk of disloyal behavior within a business network, to get access to unique competence and human capital, to transfer assets within a consortia and trans-border transactions. Licensing can be a successful way of actually *creating products*, as well as controlling *intellectual property* and *protecting intellectual property rights*.

It is indisputable that today's economy is a knowledge-based economy and most companies are aware of the fact that a substantial part of their value is in the structural form of intangible assets. A competitive advantage is to possess the ability to look beyond the concept of patents and copyright to identify other kinds of intangible assets than the ones historically considered to be such assets. Intellectual property is so strongly attached to the understanding of patents and copyright that they often are used in the same sense. A company may improve its value by identifying all intangibles and use the legal framework combined with a well defined and structured contractual approach, in order to transform these intangibles into more valuable assets. The intellectual property can be seen as the object to be commercialized or the permission to act in accordance with certain behavior, thus using someone else's trademark for instance can be the objective for a license. The license construction is a commercial transaction of growing importance. The license construction is maybe even the most important tool in order to make intellectual property available and to control such property within one's network, both when the objective is to be commercialized and to protect knowledge. A license therefore is a legal construction as well as a strategic instrument that can be used in several different ways.

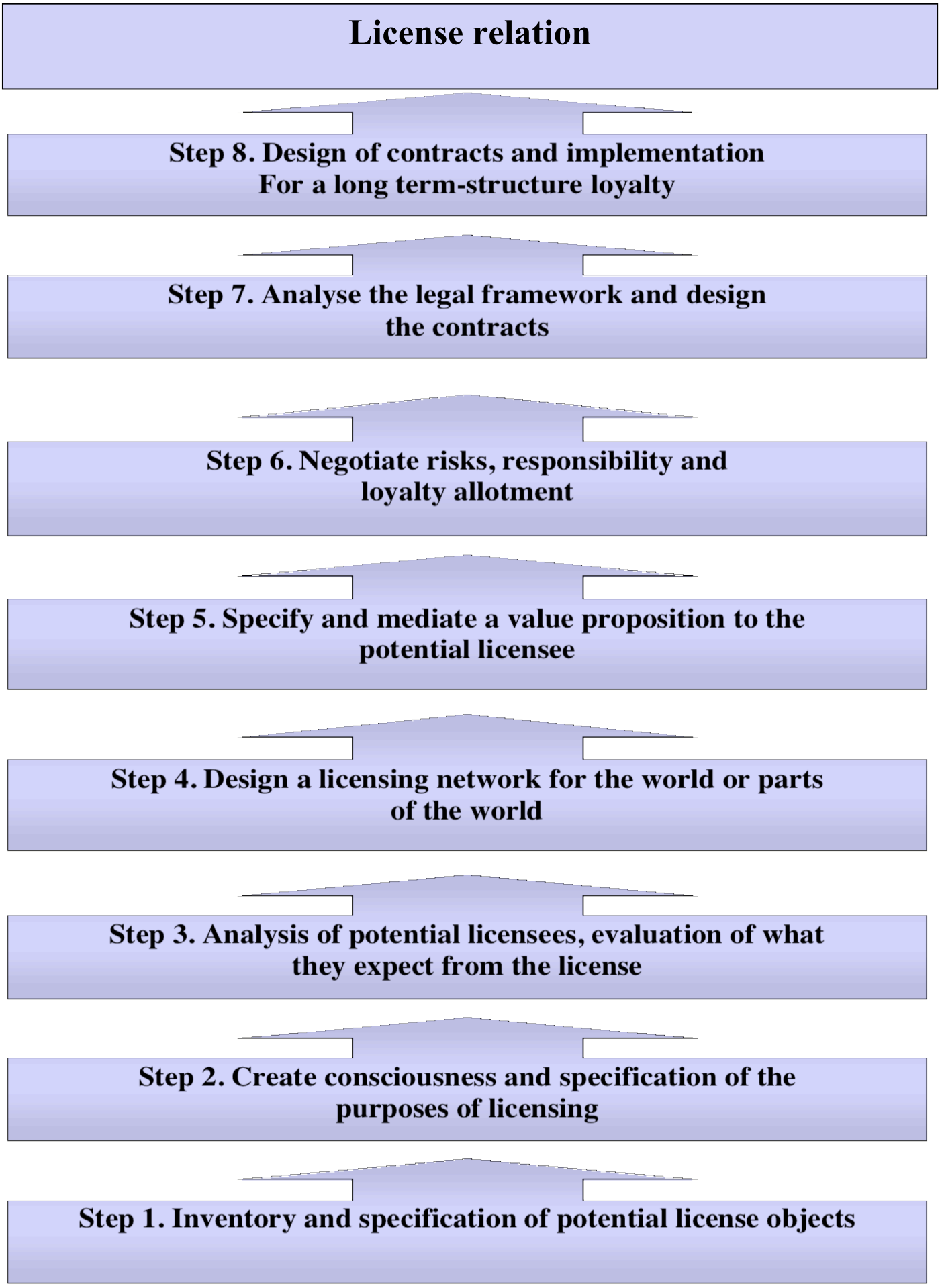
8.1. The License

In a license agreement the object or asset can remain with the licensor and the licensee is given *the right to use* under certain conditions. The license will entitle the licensee to perform actions that otherwise would be solely the right of the licensor, and the licensor will abstain from claiming infringement. Often the licensing process is considered completed when the agreement is signed, and thus all that is needed is to keep it safe from future conflicts.

However, the license agreement must be seen as part of an ongoing relation between the contracting parties. What has been decided must be implemented and communicated to everyone involved and realized by their actions. The agreement must be seen as the starting point of a long-term co-operation, that allows such flexibility that a collaboration of this kind demands. To be able to create a successful license relation the process first needs to be deconstructed and thereafter rebuilt with careful considerations preceding each step. [40]

The deconstruction of a company structure is necessary to comprehend and distinguish between human capital and structural capital in order to be able to turn intangible assets into objectified property. To license such property is to commodify and create new and better corporate structure.

[40] Petrusson, Ulf, Center for Intellectual Property studies


License relation
Step 8. Design of contracts and implementation For a long term-structure loyalty
Step 7. Analyse the legal framework and design the contracts
Step 6. Negotiate risks, responsibility and loyalty allotment
Step 5. Specify and mediate a value proposition to the potential licensee
Step 4. Design a licensing network for the world or parts of the world
Step 3. Analysis of potential licensees, evaluation of what they expect from the license
Step 2. Create consciousness and specification of the purposes of licensing
Step 1. Inventory and specification of potential license objects

8.3. Inventory and specification of potential license objects.

The first and maybe the most delicate task with the construction of a license relation is to define the object of the license in question. It must be explicitly stated in the agreement what the parties intention is regarding this issue and a thorough investigation and discussion must precede such decisions. There are two different viewpoints concerning a license construction. A license relation can be based on the *subject* and have the objective of keeping a good and prosperous relation going. Another way is to consider the license as based on an *object* and that one or many transactions take place to transfer this object.

When intellectual property is discussed people often tend to believe that this is the same thing as discussing intellectual property rights such as patents and copyrights. The concept of licensing can be used in many more situations than this and the future development of our knowledge-based economy indicates that a comprehensive understanding for the licensing concept may turn out crucial. Everything that a company considers an intangible asset can be the object of a licensing agreement. By realizing this companies will also start to realize that by treating their intangibles as assets, and therefore as potential objects of a license agreement, it will actually *create* new intangible assets, as a part of the company's licensing structure. Companies will realize that not only a database but also customer relations and customer data can be the object for a license, or maybe the use and behavior of such objects is what should be out licensed.

In some cases the license object is already accessible for the licensee and the reason for entering into license negotiations is that the alternative appears to be conflict, thus creating a litigation process and maybe the risk of being liable for damages. (See also "License as a litigation tool)

Licensing can sometimes even turn out to be *a source of income*, that companies don't generally consider, and as such actually increases the company's bottom line. For explicitly knowledge-based companies all handling of knowledge of course is part of their main business, but any company that gains necessary *consciousness*, becomes a knowledge company.

8.4. The license as a litigation tool

It is not unusual for larger companies to find that other actors on the market are infringing on their intellectual property rights. For example patented innovations and technologies, copyrights and trademarks are being copied and wrongly used by competitors, retailers and associates. This is unfortunately extremely common and has forced many companies to set up infringement detection programs. Detecting an infringer can be described as the potential origin of a conflict. It can also be seen as the discovery of a company in need of a license!

Different companies establish different strategies to handle infringements. In certain cases and for some businesses a litigation procedure is in fact the best solution. They are however costly and time consuming and not always the best option.

Providing an infringer with a license offer is another way of approaching such an issue. Instead of threatening them with litigation and lawsuit, a license offer could be considered. An offer to a major actor may even act as a warning to smaller companies and others may more easily follow.

To communicate with retailers, business associates and even parallel importers that may emerge – both authorized and un-authorized – by offering a license construction, is advantageous for many reasons. An intangible, such as a trademark, is presented and treated as a licensable object or the license is about how the licensee can behave as regards the principals branding policy. Perhaps most important, the licensor signals control and ownership

As has been verified over and over, a trademark sometimes represents enormous goodwill and becomes so well known that it possesses a value in itself. A holder of a trademark may in such situations chose to *commercialize the use* of the trademark. To grant a trademark license is to put one's trademark at someone else's disposal, which according to the Swedish trademark act VML 32 § is possible, as personal property (lös egendom), separately from the company it belongs to. This makes it possible to trade with trademarks without a connection to a specific product, service or business. Use and licensing of trademarks is often regulated in connection with retailer agreements, even though it is not self-evident that trademarks are included in such agreements. Also to remember is that from 1 January 1993 the obligation to put the trademark into genuine use has been sharpened why there is yet another advantage in some situations to let a partner license ones trademark. The use of the trademark by someone else, with the consent of the owner, shall be deemed to constitute use by the owner. A trademark right holder has the opportunity to, by licensing the right, comply with that regulation if she does not use it otherwise.

The license gives the licensee a right to, within a specified geographic area, use the trademark regarding for example commercially or informational purposes. This can lead to that, in that specified area, the licensee is the one who is associated with the trademark. It is utterly important however, to remember, that when the license relationship ends, the trademark rights follows the product, if nothing else is regulated contractually.

The trademark follows the product!

According to Swedish law there are no formal demands for how to draft a license agreement. The parties are free to decide what they find necessary in regards to agreement terms. Issues regarding *linguistic usage* of the trademark are recommended to regulate. The trademark might need to be modernized and changed as time goes by and it is important that the licensor can force the licensee to use it in its modified form. An *obligation to use* could be necessary as well, which is not the case if not regulated. Division of possible *costs* that may occur, for instance costs for renewing the registration of the trademark and litigation costs for processing if a third party is infringing, must be regulated. In what situations the trademark may be used is equally important, such as selected marketing events and commercial activities, so called *field of use-clauses*.

If a licensee uses the trademark differently from what is permitted in the agreement, this is to be considered an infringement. (VML 34 § 2 section) Rules of sanctions and damages can then be applied.

The legal regulations on the area of license agreements are optional, meaning that the parties have great freedom to create tailored agreements. Breach against an agreement is an infringement of the law.

8.6. Exclusive, non-exclusive and sole license

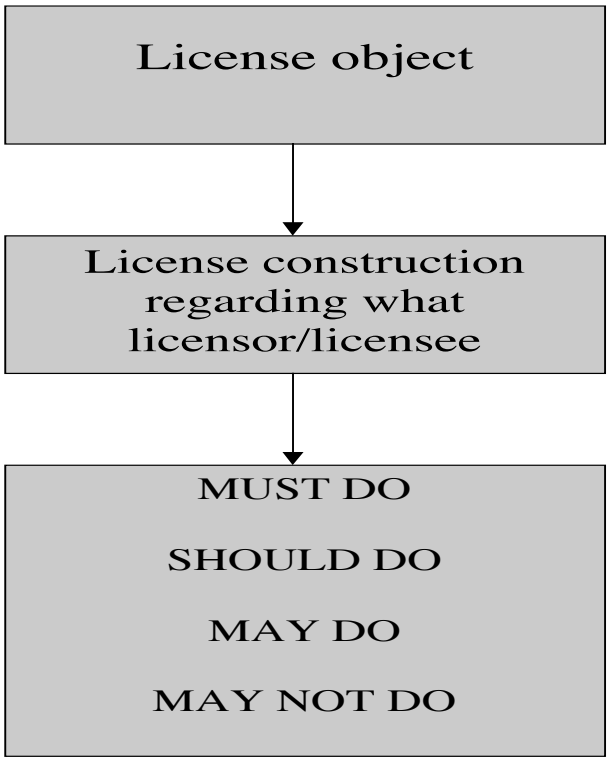
The licensee can receive a *non-exclusive license*, which means that the licensor puts the trademark at his disposal but not exclusively to this certain licensee. The licensor retains the right to give anyone else the same right to use the trademark and may also exploit the trademark himself in the area.

An exclusive right to use the trademark in a specified geographic area is given by an *exclusive license*. The licensor thereby is bound not to give anyone else the right to use the trademark in that area and will not use it himself either.

The licensor also has the possibility to provide a *sole license*, whereby the licensor reserves the right to use the trademark herself but apart from that the licensee gets an exclusive right.

An exclusive license is naturally more valuable for the licensee as well as the right for the licensee to sub-license to any third party. Different combinations of licenses exist and they may be designed for each situation specifically. Standardized agreements in this area are not common. Remember that the objective of the license is to create a framework for how the licensee may dispose of the licensed object, the trademark. If the licensee steps outside the set boundaries of the agreement it should constitute ground for damages and other sanctions. An exclusive license could be changed into a non-exclusive license if the specified conditions are not complied with. The license entitles the licensee to certain use but it is important to remember that any obligations to use must also be stated in the agreement, if that is desired. This could be of utmost interest if the licensee for instance also provides other competitive products or services.

In order to preserve the goodwill of a trademark, the licensor sometimes puts explicit demands forward in a license agreement. It could be other products or services that must be provided in connection to the licensor's products and together with the trademark. Such conditions that forces the licensee to certain behavior, so called tie-ins, needs to be used with care because of their impact on competition and free movement of goods.



8.7. Cross license constructions

Clauses in a license agreement that regulates the parties right to use each other's developments are usually called grant back-clauses. Closely related to such clauses are agreements of cross licensing, when both parties give one another permission to use their respective rights. In some situations the objective for the parties is to *exchange* knowledge and for that cross licensing can be the ultimate solution. Often the main obligation for a licensee in a license relation is to pay, normally some kind of royalty or maybe a lump sum. Other ways of performing this obligation is to provide the licensor with a license, in which case the parties enters into a cross license relation. Cross licensing decreases or eliminates payment. The retailers' use of the trademark is a prerequisite for them to be able to sell any products. This relationship between the producing company and the retailers is in fact a license relationship and the transfer of customer data from the retailers to the producing company can in fact be seen as a grant back. Both the concepts of cross license and grant backs are considered accepted ways of exchanging knowledge or other kinds of intangible assets. However, to act in accordance with these, in this situation, rather antique formalistic conceptions may in our case create the misapplication that the customer data in fact belongs to another party than the producing company, and therefore should have the possibility to make an offer to the producing company for using the customer data. It's our opinion that nobody but the producing company is the rightful owner and controller of the customer data collected, and therefore only the producing company possesses the possibility to put any such offers forward.

It is possible for the producing company to regulate the transaction and/or use of customer data in a license agreement that is created to communicate to a party how to use the brand, but it is not our recommendation to place customer data on an equal level to what the licensee shall perform in the relation. Such a solution would counteract the fact that the producing company is already the rightful owner of said customer data, which instead has to be emphasized.

8.8. Most favored constructions

Other licensees might demand equal treatment without giving any monetary credit to the value of cross licensed property and grant back clauses and so on. Some will try to achieve a *most favored clause*, which means that they would be entitled to the same terms as the initial licensee or any other licensee with a better deal. There are however important to remember that the risk of litigation process will increase due to, among other things, competition law. Using different kinds of license constructions for the same license object to different licensees may cause problems and be ground for litigation. In cases like this one needs to be extra careful as the construction may cause problems not only from a contractual point of view but also, as mentioned, from an anti trust regulations angle.

To construct a license agreement is a work of art! Both parties must find themselves in a winning position, thus both parties must gain something from the relationship. The court and judges must be satisfied, in any future, potential litigation, such as for example an anti-trust issue or an infringement suit. To formulate an internal strategy on company objectives and desired control is a good start.

9. Conclusion

Companies of today are acting on a global arena, not only via daughter companies and independent business partners with which they have a contractual relation, but also due to the Internet. Most would agree that we in fact have entered into a completely new era where information and knowledge based business is becoming more and more important. The world of business is going through a structural transformation that will place new demands on a legal framework and experienced business methods. This globalization and diversification of the business increases of course the market and creates many possibilities, but it also increases competition, which makes it important to create ways of having a close relation to customers and to ensure the control over the customer data. A company can transform business and customer relations into objectified structural capital and by doing this create an increased value of the intangible assets in the company. To achieve this companies must be aware of other kinds of intangible assets handled by the company, and make them collaborate with each other to gain synergy effects. Intellectual property acts as a mean of protection and also in situations of bargaining and other marketing situations. This thesis has tried to show how self-assured management can deconstruct and do careful inventories of their business in order to be able to create sustainable structures. Furthermore the thesis has tried to describe the difference between database *content* and *structure* and how these different concepts can, and must be, attended to and protected by different legal tools and concepts.

The main issues that we have investigated have been on what basis personal data can be processed in order not only to comply with the present regulations, but also to ensure that it can be used in a business effective way, and how the customer database can be legally and contractually protected while at the same time creating retailer loyalty. The three pillars that we have built our strategy on can be said to be:

- How to handle customer data and customer relations in relation to personal integrity regulations.
- How to protect content and structure in relation to business partners and potential infringers.
- How to establish ownership and create a solid control position by using the trademark and a contractual construction.

As there is no such thing as a simple legal answer to these issues, a company by itself must try to define which legal tools it can use in order to create the structures. The legal tools that we are referring to in this thesis are primarily PUL for building value and customer acceptance in the customer database. In our opinion PUL should not be seen as an obstacle for achieving certain goals, but as a mean of actually creating further customer goodwill and acceptance. To comply with a legal act that is aiming for consumer protection most of all is for a company to communicate, to existing and potential customers, the already existing values that the trademark possesses. It is also an additional signal to business partners and others concerning who the rightful owner of the customer data and customer relation is - the mother company.

The Database Directive and the Swedish Copyright Act are useful legal tools for securing the database structure and the Swedish Trade Secrets Act for securing the content. By using these regulations in combination with the trademark right that follows with the trademark, the mother company is in a superior negotiation position to communicate their opinion on how the legal situation shall be interpreted.

By using the trademark to communicate that it is the trademark as such that has built the value in the customer database, meaning that without the trademark the customer data base would not exist, and enhancing this with a licensing structure will secure the control of future, potential personal data as well as customer data already existing.

It is our opinion that this thesis only has begun to show how difficult, but still extremely important, it is for companies to recognize the complexity of these matters. Discovery of the need for an inventory of the company in this field and finding the proper questions to ask is a major first step. However it must be emphasized that this can only be considered the tip of the iceberg. A more complete investigation and analysis of a company's structure and assets must be both wider and deeper and most of all ongoing. We like to consider it a journey, where further knowledge on how different areas mix and interact, such as the traditionally very strict legal area and the more changing area of modern business management, will help you become more competitive and profitable. We will therefore recommend readers to continue the process that we hope this thesis has helped to initiate.

10. List of references

Written sources

Barlebo Wenneberg, Sören: ”Socialkonstruktivism – positioner, problem och perspektiv”, Liber, 2001
Cheeseman, R. Henry: ”Business law: Ethical, international & e-commerce environment”; Prentice Hall, 2001
Jensen: Nordiskt Immateriellt Rättsskydd (NIR) 1999
Koktvedgaard/Levin: “Lärobok i Immaterialrätt”; Norstedts Juridik, 2000
Petrusson, Ulf: ”Patents as Structural Capital”, 2002
Robert F. Reilly, Robert P. Schweihs: Valuing Intangible Assets, McGraw-Hill 1999
Öman/Lindblom: ”PersonuppgL – en kommentar”, Norstedts juridik, 1998

Government publishing

C-355/96; 16 July 1998
SOU (1997:39)
Prop. (1997/98:44)
Prop. (1999/00:11)

Oral sources

Andersson, Lars; PhD student Chalmers University of technology
Clancy, David; Strategic Policy Officer, Information Commissioner’s Office, UK
Wallin, Elisabeth; Data Inspection Board, Sweden
Wiklund, Anders; Data Inspection Board, Sweden

Internet

www.wipo.org
http://oami.eu.int/
www.regeringen.se