BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

Brochures

Legal Issues of Electronic Commerce-

A Practical Guide for SMEs

ECLIP

Executive Summary

These brochures are a simple reference document to provide guidance on the legal issues relating to e-commerce in Europe with particular emphasis on the legal framework being approved by the institutions of the European Union. The brochures do not intend to provide an in depth analysis of all the issues on a state-by-state basis. Instead some of the main considerations for Internet Service Providers (ISPs) when establishing a web-business are considered. These brochures are targeted especially at smaller and medium-sized undertakings seeking to sell goods and services over the Internet on a European wide basis.

The brochures contain summaries, drafting guidance, checklists, tips, links to useful websites and other practical information. The approach is to distil and present the key legal issues for a non-legal audience. It is hoped that this will enable small and medium-sized undertakings to understand the legal considerations and legal pitfalls in e-commerce. The brochures should assist these businesses to put the relevant questions to their legal adviser and thereby to improve the client-adviser relationship. However by necessity the brochures are of a general nature only and cannot replace specialist legal advice for specific problems.

The approach taken in the brochures is not so much to provide a mere summary of the law for which a legal textbook may be more useful. The approach has rather been to provide specific guidance as to what the undertaking has to keep in mind when trying to achieve specific goals and steps in setting up an e-commerce business.

In the first phase, the setting up of a website, the Internet Service Provider (ISP) will have to get an Internet connection. It needs to choose and register a domain name suitable to his business. Before registering a domain name he should, however, be aware of the trademark issues relating to the use of certain domain names. Also infringement of trademark protection is relevant here. This is dealt with in chapter 1.
Next, the business will have to choose content for his homepage, pictures, texts, logos, or other multimedia devices. It should be aware that these documents may be protected and that it needs to hold the relevant rights. The business might want to offer a service on the Internet which includes the creation of a web page, a whole site and/or an electronically accessible database. Furthermore contracts with the web designer will have to be considered, as well as hosting and access agreements. All legal aspects of designing a website will be briefly addressed in chapter 2.

The third step is designing the web-contracting process, taking into account consumer protection issues. Chapters 3 and 4 deal with the contracting process, the information which should be given to a consumer, advertising communications and also the use of special trust mark schemes, enhancing branding and consumer confidence.
The next step relates to the payment methods to be selected by the supplier and its contract with the issuer, be it a credit card company or an electronic money institution, including the relevant issues of security and data protection. This is dealt with in chapter 5.
Chapter 6 then explores principles of taxation in e-commerce. These considerations are important for tax planning as well as for tax compliance issues. Chapter 6 includes practical reference to define the permanent establishment for income tax purposes as well as the

treatment of online products as goods or services. It also deals with the question where the VAT should be collected and it also provides guidance as to how to comply with tax law when engaging in on-line transactions.
When engaging in electronic commerce activities, including the various steps of the contractual process, companies will have to collect data. Special attention therefore needs to be paid to data protection regulation and this is dealt with in chapter 7.
Finally, disputes may arise in the e-commerce context. Because of the problems associated with cross-border litigation, the last chapter of the brochures (chapter 8) describes various online alternative dispute resolution systems, which may be of assistance to small and medium sized businesses.
This brief introduction shows that various legal issues must be considered. They arise in all phases of electronic transactions including the process of preparation. All types of e-businesses may face new legal requirements, which they have not yet been aware of.

TABLE OF CONTENT **Page**

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 1

Choosing and Registering a Domain Name

CHAPTER 1

1. Choosing and Registering a Domain Name

One of the first topics that has to be considered when starting an online activity concerns the choice and the registration of the respective internet domain. While the choice and registration of the domain name itself will mainly be driven by marketing reasons, some legal implications should also be considered. In addition, this chapter will provide some advice as to how to protect one's own domain once it has been registered.

1.1 General Information on Domain Names

Domain names provide a system of easy-to-remember Internet addresses, which can be translated by the Domain Name System (DNS) into the numeric addresses (IP Numbers) used by the network.

1.1.1 Structure and Types of Domain Names

Domain name addresses are easy to remember and therefore simplify the identification of computers on the Internet for communication. All domain names follow a hierarchical structure, consisting of at least two components called level domains which are separated by dots. The top-level-domain (TLD) is the component on the very right of the domain name followed on the left side by at least a second-level-domain. On the left more sub-domains, up to three, may follow. Two different sorts of TLDs exist:

International or generic TLDs (gTLDs) refer to the kind of institution holding the website, e.g. the TLDs ".com", ".org", ".net", ".edu", ".int" and ".gov" and the new TLDs ".aero," ".biz", ".coop", ".info", ".museum", ".name" and ".pro" that have been introduced by the ICANN (Internet Corporation of Assigned Names and Numbers) in November 2000.

Country-code TLDs (ccTLDs), on the other hand, refer to a country, e.g. ".uk" for the United Kingdom, ".fr" for France and ".de" for Germany. In addition, the TLD ".eu" has recently been introduced by the European Union. For businesses especially the ".com"-domain is of

special relevance due to its international flavour. For companies which focus on a national market country-code TLDs provide nevertheless a good alternative.

1.1.2 Domain Name Registrars

Domain names are allocated by registrars. For country-code TLDs there is usually one central so-called Network Information Centre (NIC) which registers the domain names under the country-code TLD. The generic TLDs had for a long time also been allocated by one centralised body, Network Solutions Inc. In 1999 a new shared registration service has been introduced to create competition in the area of generic TLD registration. A number of new registrars are now able to provide the registration service for the named generic TLDs as well.

TIP:
For a list of ICANN accredited registrars please see:
http://www.icann.org/registrars/accredited-list.html

Each NIC registers the domain names according to the registration guidelines it defined for the centre. These guidelines still differ considerably. Also the fees charged for domain name registration and administration vary. Mostly the NICs register second-level-domains according to the request of the applicant, further sub-domains may be created by the holder of the domain under his own responsibility. In some countries such as the United Kingdom the applicant has to choose a generic second-level-domain, such as “co.uk” for commercial use or “org.uk” for non-profit organisations, and only the third-level-domain is distributed according to the applicants demand. A detailed system of subdomains has also been introduced by the registration authority of “.fr”, AFNIC.

TIP:
The UK registrar, Nominet can be found at: http://www.nic.uk/
The French registrar, AFNIC can be found at: http://www.nic.fr/
The German registrar, DENIC can be found at: http://www.denic.de/

The person wishing to obtain a domain name should contact an Internet Service Provider (ISP) which will then be his agent in the application process. This is often the most

convenient way for the applicant as the ISP has usually already been charged with the procurement of the IP number and is also offering further services. Furthermore the intervention of an ISP is often requested by the NICs. Some NICs, however, also offer direct registration without ISP intervention.

1.2 Possible Domain Name Interference with Trademark Rights

A trademark is a sign which is used to identify and distinguish the goods and/or services of one person, from the goods and/or services of others, and to indicate the source of the goods and/or services. As such the sign needs to be distinctive. Merely descriptive terms do not qualify for trademark registration unless they have acquired distinctiveness in the concrete context. Trademark protection is usually achieved by registration of the sign at a Patent and Trademark Office (PTO). Especially countries in northern Europe also provide for a similar protection to unregistered trademarks if certain additional prerequisites are fulfilled and the signs have acquired a secondary meaning. Also famous or well-known marks benefit from an - often extended - trademark protection in most countries although not registered in the concrete country.

Domain names, as they are easy to remember and often even easy to guess have become a valuable marketing tool. While designing a website is rather simple the crucial point for the success of a website is how many people will find and visit it on the Internet. One important factor in this respect is the use of a domain name which is easily associated with the company. A company therefore wants to obtain a domain name which corresponds best either to its trade name or trademark. That is why domain names have achieved a business or organisation identifying character for the great majority of websites.

Domain names in the generic TLDs as well as names in most country-code TLDs are however not granted after verification of whether the applicant has a right to the name he wants to register. Domain names are usually registered on a “first come, first served” basis. Anyone can therefore basically register any kind of domain name.

1.2.1 Bad Faith Registration and UDRP

The registrars' practice of granting domain names to applicants without verification of a right to the domain name has led to a situation in which some persons - often referred to as cyber-squatters -, registered a number of domain names which were associated with other companies with the intention to resell these domains to the company.

In response to such cybersquatting, the ICANN created the Uniform Domain Name Dispute Resolution Policy (UDRP), a dispute resolution process for such bad faith domain registrations in 1999. The UDRP provides for a cheap and fast procedure in domain disputes concerning generic TLDs. In contrast to other voluntary dispute resolution procedures, all domain holders have to submit to the UDRP when registering a domain name. In the procedure, the complainant files his complaint at one of four dispute resolution providers.

TIP
The dispute resolution providers for generic top level domain name disputes can be found at:
http://www.icann.org/udrp/approved-providers.htm

A panel of arbitrators decides about the conflict on the basis of the written complaint and a statement of the opponent. The complainant has to bear the costs of US $ 1500 – 3000 for the procedure which is generally conducted within less than two months (unless the defendant chooses to have the dispute solved by a three member panel). In order to be successful, the caimant has to establish that

(i) the opponent is using a domain which is identical or confusingly similar to his protected trademark
(ii) without a right or a legitimate interest and
(iii) has registered and used the name in bad faith.

Bad faith is generally assumed if the domain is registered in order to sell it to the trademark owner, if it is registered primarily for the purpose of disrupting the business of a competitor or if it is used to create confusion in order to attract internet users to a homepage of one's own.

In case of bad faith registration by the opponent, the respective domain registrar is obliged to obey the panel‘s order to transfer the domain to the complainant or at least to delete it without any further governmental execution. Nevertheless, both the claimant and the opponent are allowed to take further legal steps before the regular courts within a period of 10 business days. However, the UDRP can be regarded as a very helpful procedure in case of bad faith domain registrations.

1.2.2 Possible Other Trademark-Related Domain Name Conflicts

Conflicts between trademarks and other rights to signs do not only occur where bad faith registrations by a cyber-squatter have been made. Signs which usually co-exist peacefully suddenly collide when it comes to domain name registrations. This is due to the fact that two of the main principles of trademark law are contradictory to the domain name system.

1.2.2.1 Principle of Territoriality

The first one is the principle of territoriality. It says that trademarks are national by nature. Trademark protection by a national Patent and Trademark Office is only granted for the territory of the country in which the sign has been registered. If protection for a further country is desired the trademark holder basically needs to apply for a registration at the PTO in that country.

While Country Code TLDs refer to a certain country the domains are nevertheless accessible from all over the world due to the borderless nature of the internet. Generic TLDs do not even refer to a certain territory but are international by nature. Therefore persons which hold identical signs in different countries would all like to obtain the same “.com”-domain. While in one country the domain would be associated with the company using the sign in that country, in another country a different company would be identified by the same domain. This company might see his trademark rights infringed by the use of the domain by a different company.

1.2.2.2 Principle of Speciality

The second principle which creates problems in relation to domain names is the one of speciality, according to which a trademark protection is granted for certain categories of

goods and services only. Basically, a trademark infringement can only be established if the protected sign is used in relation to products or services which are identical or similar to those for which the trademark has been registered.[1] The principle of speciality also means that an identical sign can be registered for certain goods and services if the sign which is already protected is protected for dissimilar products and services only.
An exception to the principle of speciality is made in most EU Member States in relation to well-known trademarks or trademarks with a reputation. These qualified trademarks benefit from an extended protection beyond the field of similarity, if the use of the sign by a third party takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark.[2]

The principle of speciality leads to severe conflicts in the online world. While the same sign can be registered for several different goods or services in a country from a trademark law point of view, all holders of this particular sign would want to obtain the same domain name which exists only once as domain names necessarily have to be unique in each TLD.

1.3 Choice of TLD

The first choice that needs to be made is the one of the TLD. In order to avoid customer confusion it may be reasonable to register the domain in all TLDs which would generally be associated to the company, which means the country-code TLDs in all countries in which the company is acting or is planning to expand its business to and the relevant ".com"-domain if the company is not purely national. Registering the same second level domain in all relevant TLDs also helps to eliminate the risk that a different company will use a domain name which is associated to one's business so that it may be very difficult to obtain the domain later.

1.4 Choice of Second Level Domain

Secondly, a suitable second level domain - or third level domain in TLDs which provide for generic second level domains - has to be found.

[1] Art. 5 para. 1 a,b EC directive 89/104/EEC.
[2] Optional provision in Art. 5 para. II EC directive 89/104/EEC.

Basically, a company has two options, either to register a domain name which corresponds to the sign by which it is best identified (trademark, trade name, abbreviation of such, other kind of business identifier) or to chose a generic term which Internet users may type in when looking for a certain product and which might stick more easily in the users mind, if the business name/mark is not yet very well known. In some country-code TLDs it is, however, not possible to register such generic terms according to the registration guidelines.

The registration of generic terms has some disadvantages also from a legal point of view. Domain names as such do not grant an absolute right to the sign. If a competitor e.g. was to register a confusingly similar generic term as his domain name or the same generic term in a different TLD it is difficult to take legal action against such registrations. Only in cases in which the generic term has achieved a secondary meaning and is therefore identified with a concrete business or where considerable good will is at stake actions based on unfair competition law or passing-off may be successful.

If the domain name, however, corresponds to the company's trademark or trade name it indirectly benefits from the protection granted to these signs and even of the priority which they already had in the real world.

In order to avoid confusion with other signs which are used for different types of products and services it should be considered to include an indication of the type of product or service which are to be offered on the website in the domain name, e.g. "www.miller-banking.com". This may limit the risk of being exposed to claims by other parties which hold the same sign for different products and services.

In addition it may be considered to register any different spellings or similar spellings in order to avoid a competitor associating itself with the business.

1.5 Prior Trademark and Domain Search to Avoid Conflicts

Before definitely deciding which domain name to choose, a search should be effected on the one hand on pre-existing trademarks with which the domain name could interfere and also

with other domain names which might be confusingly similar. With regard to domain names a "whois"-databank search possibility is regularly offered by registration authorities in their TLD for free whereas trademark searches might require professional assistance by a lawyer familiar with that area of law.

1.6 Dealing with Prior Registrations of the Desired Domain Name

If the desired domain name is already taken, it should be examined whether the user of the domain appears to have a legitimate right to the use of the sign.

If no, it may be considered to challenge the domain name registration through the ICANN UDRP addressed above (see sec. 1.2.1) in case of bad faith registration or through legal proceedings before the regular courts.

While many trademark holders have been successful in legal proceedings it still has to be emphasised that not any domain name use has to be considered as infringing a certain trademark. Especially where the website contains information which does not bear the risk of confusion or association with the trademark, courts will probably rather rule in favour of the domain name holder. It might therefore be easier to turn to a different domain name, again by adding e.g. the products or services offered than taking the financial risks of a legal action. At least for SMEs which usually do not have a very strong trademark this will often be the better solution. Before taking legal steps in order to obtain a registered domain from the actual owner it should always be considered to negotiate the transfer of the domain.

If the domain name holder also holds a right to the sign which constitutes the domain name, legal proceedings will rarely be promising. Chances are better if the trademark on which the claimant bases the dispute is strong and well-known. Some disputes have also been based on the argument that the challenging trademark benefits from priority in the off-line world.

If the two protected signs which clash in the domain name are not used for similar products or services courts will probably already reject a trademark infringement as no risk of confusion

or association is given and therefore the question of priority does not even need to be considered.

1.7 Protecting One's Domain After Registration

Once a domain name has been registered, a company may see the value of its domain name endangered by the latter use of a similar domain name or the registration of an identical or similar trademark. Such similar domain names or trademarks may dilute the reputation of the website and the products/services which are related to it.

If the domain name corresponds to the company's trademark or trade name, a claim against a new, conflicting domain or trademark should be based mainly on these rights. In claims against a new trademark the domain name as such has in several cases also been accepted as an earlier right constituting a ground for refusal of the trademark registration. In claims against similar domain names the prior domain name can in most countries only be evoked on the grounds of unfair competition or passing-off. Some countries, e.g. Germany, grant a trademark similar protection also to other business identifiers if they are sufficiently known. In this exceptional case a claim can also be based on this right achieved in the domain name. Again this situation shows that the registration of a domain name which corresponds to other protected signs of the company is very favourable to achieve a high standard of protection in relation to the domain name.

In general it is recommended to regularly check whether critical domain names or trademarks have been registered in order to be able to react early, e.g. in the period in which removal of a new trademark can be achieved by an administrative proceeding or in which the new domain name holder has not yet acquired any good will in the domain.

1.8 Trademark Registration of the Domain Name

In order to achieve a stronger protection of their domain name, a number of companies started to register their domain names as trademarks.

Often such registrations will be of little additional value. If the distinctive part of the domain name corresponds to a trademark or the trade name of the company the domain name

indirectly benefits already of the protection of these signs. It also has to be kept in mind that any trademark registration is liable to revocation if the trademark has not been used for a period of five years. It is probable that the sole use of the sign as a domain name will not satisfy the requirement of genuine use. Only if the domain name is used in closer relation to the service or goods for which the trademark has been registered, e.g. on packaging, on the website as name of the service etc. this will be regarded as sufficient use of the trademark. The main value of a trademark registration therefore lies in the first five years in which protection is granted to the sign even though the trademark holder has not yet made any use of the sign.

Companies that nonetheless would like to register their domain name with a Patent and Trademark Office, should be aware that domain names can only be registered as trademark if they fulfil all prerequisites of trademark registrations, which means first of all that they need to be distinctive. As the prefix “http://www.” and a TLD are not distinctive, they cannot add to the distinctiveness of a sign. Furthermore, the company has to decide in which classes of goods and services the domain name is registered. Basically, the domain would need to be registered in the classes of goods and services in which the company is doing its business. The mere advertisement of one’s products on a website will not be sufficient to qualify for a service class. On-line-advertisement for customers may however be regarded as a telecommunications service. The choice of the right classes of goods and services should be discussed with a local lawyer who follows the national development in this field.

1.9 CHECKLIST FOR CHOOSING AND REGISTERING A DOMAIN NAME

1. Step **Choice of the top-level domain: where to register?**

- It may be advisable to register in all the national top level domain registries of the countries where the business is acting or planning to expand and also to register the top-level domain .com - see ICANN at www.icann.org. This would prevent any other business from taking the domain name later.

2. Step **Choice of second level domain and name: what to register?**

- A suitable generic second level (e.g. co. or org.) must be chosen in the countries providing for these.
- Also the identifying domain name must be chosen. This will be usually the business' trade name or trademark. In addition any different spellings or similar spellings should also be registered to avoid a competitor associating itself with the business.
- Also it should be considered whether to register a generic name, which the user will more easily remember. However some registries do not allow the registration of generic names. Also it should be kept in mind that generic names will not be protected unless they have achieved a secondary meaning.

3. Step **Trademark and Domain Name Searches**

- It will be necessary to carry out a trademark search to insure the chosen name does not conflict with a trademark.
- It will also be necessary to carry out a domain name search to see whether the name is still available and to avoid conflict with similarly spelt names. This is usually offered by the registration authorities
- If the same or a similar name is registered as a domain name or trademark one way to avoid confusion would be to add an indication of the type of products/business in the domain name, e.g. www.miller-banking.com

4. Step What if the preferred domain name is already registered?

- The registration could be challenged through administrative dispute resolution proceedings offered by the registration authority (ICANN UDRP)
- However, to do so, there is often a requirement to show that the name has been registered in bad faith
- The registration could be challenged by legal proceedings based on trademark (or other right) infringement. However it should be emphasised that not every domain name use is an infringement.
- Before taking any steps to challenge the domain name, it should be attempted to negotiate a transfer
- It might therefore be easier and cheaper to turn to a different domain name.

5. Step Trademark registration of the newly acquired domain name

- If not already protected as a trademark, the domain name to be registered should be registered as a trademark in order to achieve stronger protection.
- However is has to be kept in mind that trademarks can only be registered if they are distinctive. The top level domain suffix and http://www. are not distinctive.
- The classes of goods/services in respect of which the mark is registered should be discussed with a local lawyer.

1.10 TRADEMARK INFRINGEMENT CHECKLIST

Protection of your mark

Is your mark protected in the country of use?
It can be protected by:

- Registration in that country
- Trade name protection, unfair competition law, passing off
- Is your mark a famous international trademark?

IF YES

Use of the respondent's mark

Is the mark used?
Is it used in trade or commerce?

Examples: use in advertising, on packaging, on products,
as domain name…..

IF YES

The relationship between your and the respondent's marks

Is the respondent's mark identical/similar to your protected trademark?
AND
Are the goods/services identical/similar?
Is there a likelihood of confusion?

OR

Is your trademark well-known?
AND

- Does the respondent's use of the mark take unfair advantage of your trademark? OR
- Is the use of the mark detrimental to your trademark?

IF YES **IF YES**

Does the respondent have a better right in the mark?

Does the respondent also hold a right in the mark and what kind of right is this (e.g. trademark, right in the name, copyright)?

IF N(Does the respondent's right benefit from priority?

Is the claim barred for any other reason?

- You must not have been aware of and acquiesced in the respondent's use of the mark (for a period of at least five years or shorter in some Member States).
- The mark complained of must not be the personal name or address of the respondent - it cannot be prohibited to anybody to use his name and address in commerce.
- You cannot rely on your protected mark to prevent an import of goods under the mark from another Member State, if the goods were lawfully marketed there under the trademark (principle of exhaustion), unless the goods have been altered.
- Your claim also fails if your trademark has not been used for a period of five years. The respondent may use this as a defence.
- Your claim must not be barred because too much time has elapsed since the infringing act (prescription)- this time differs between the Member States.

IF NO

=> YOU MAY HAVE A VALID CLAIM

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 2

Legal Aspects of Designing a Website

CHAPTER 2

2. Legal Aspects of Designing a Website

After the registration of a domain name, a company has to design and insert content on the webpage it wants to offer to internet users. In the context of website design, there are numerous legal issues that have to be considered in advance.

The creator of a typical webpage usually wants to include a number of Intellectual Property protected materials, such as texts, photos to illustrate the text, graphics or pictures, some accompanying sound files, hyperlinks or icons programmed in a scripting language. Furthermore, the company may want to make protected material such as software, music files, or movies available on its website for downloading. The is a general misperception that material "freely available" on the Internet can be used without obtaining any permission. Unfortunately and as explained further below this is not true.

On the other hand, if the website owner is the rightholder in the materials, he may want to know the scope of protection offered by Intellectual Property laws and how he is able to enforce his rights against infringing use.

If he intends to use materials provided by third parties, he needs to determine whether the material is protected by intellectual property rights and - if so - how to obtain the necessary licences for online utilisation of the material.

2.1 Intellectual Property (IP) Questions concerning the Content offered on a Website

A company trying to establish an internet presence needs – after having reserved a specific internet address (i.e. a domain name) – to build up a website on which the content the

company wants internet users to access is presented. When offering content on a company website, the company has to be aware that different kinds of materials may be protected by several intellectual property rights (IPRs) and that online utilisation of such material will usually require the authorisation of the rightholder. On the other hand, the company may just as well benefit from intellectual property protection as far as their own materials are offered online.

In the following, the different aspects of copyright and related rights protection with regard to the establishment of a website are described. Each section contains at the end concrete recommendations for companies developping an online presence.

2.1.1 IP Protected Content

Almost all of the different materials which may be included on a website can be subject to copyright or related rights protection: (Literary) text such as articles, pictures or images, photos, movies, music and even collections of information (databases).

Whether copyright protection applies to any of these materials depends – since countries have different concepts of copyright protection – on the national copyright law applicable to the concrete case: Basically all jurisdictions world-wide agree that the applicable copyright- or related rights law is the one of the country/jurisdiction for which territory copyright protection is sought, i.e. for which countries' territory a copy- or related rights infringement is claimed. For example in the case of an unauthorised distribution of a CD ROM containing protected software in the USA the alleged infringement has taken place in the USA and thus US copyright law applies.

Unfortunately, in the internet environment the determination of the applicable law is more difficult: As the material accessible on a website can be viewed from any internet connected computer world-wide, the place of an alleged infringement by placing protected material online could be understood to be all countries where the infringing material can be viewed and therefore all copyright or related rights laws could be applied to the case. Neither existing laws, court decisions nor legal scholars have come up with a common solution to this problem.

Despite this problem, however, one can at least be sure that the copyright law of the country or countries to which a website owner directs or targets his online activity (e.g. the country to which inhabitants he offers his goods or services via the internet) will be applicable. This law then decides on the question whether the content used on the companies website is protected by copyright or related rights.

In the following, a short overview of the conditions for copyright and related rights in the EU member states shall be given.

For some areas of copyright, such as the protection for software and databases (i.e. collections of information such as a list of hyperlinks), harmonised laws imlementing certain EU Directives exist. In these areas the conditions for protection are the same or very similar in the EU Member States. The material in question needs to be the author‘s own intellectual creation. This requires for once the creation of the software or database by a human being. Further, the material has to be the result of that person’s own intellectual creation. Sufficient is the showing of a minimum of individuality or creativity (with respect to databases this has to lie in the selection or arrangement of the data). Ineligible for protection is only totally trivial material which does not even contain a spark of individuality or creativity. Therefore, copyright protection can be considered as the general rule, especially for software. Finally, databases are – next to the copyright protection described above – also protected in case they are the result of substantial investments of time, money or labour in collecting, verifying or presenting the data (so called „sui generis“ protection).

For the other protectable materials such as texts, images, photos or music the conditions for protection vary from member state to member state. In some countries a certain level of creativity is required in order to enjoy copyright protection (e.g. Austria, Germany, Norway and Sweden). In other countries the material must be a personal intellectual creation (France, Belgium, Italy, Denmark Finland). Still others require only that the achievement must be original (the UK, Ireland, Greece, Portugal, Spain and the Netherlands). The main difference lies in the amount of creativity required for protection.. To be on the safe side, the company utilising protectable material should presume that the required intellectual effort or amount of creativity is rather low and should therefore use the material only with permission of its

creator or rightholder. Apart from these conditions copyright protection does not require formal acts such as a registration or a copyright notice (the „©“ sign), it is rather granted as soon as the protectable work is created (this applies also to the USA and Japan).
With regard to websites containing protectable content one has to add that the webpage as such may – depending either on an creative selection or arrangement of the content or an substantial investment in collecting, verifying or presenting this content – be protected by copyright or related rights as a database (i.e. apart from the protection offered to the different materials displayed on the website).

→ A company establishing a website should therefore check carefully whether it has obtained the necessary rights (see below sec. 2.1.3) for all the third party material which could be subject to copyright protection. The fact that the material is "freely available" on the Internet does not mean that there are no thrid party rights attached to it. It should – as a general rule – assume that most of the material described above will be protected by Intellectual Property laws and therefore refrain from using any of this material without explicit permission.

→ If the company uses its own material which meets the criteria for protection (see above) it should include a short copyright notice such as “© 2001 by John Doe” or ”The content of this web page is protected by international copyright laws. Any unauthorised utilisation of this content infringes applicable copyright laws and will not be tolerated“ on the webpage or connected to the copyrightable content (e.g. at the beginning or the end of a text or under a picture). In case such notice appears on the copy, in a copyright infringement suit in some countries a defence cannot be based on the assertion that an innocent infringement occurred. Also, in most European countries it is presumed that the person mentioned as the author on the work is in fact the creator of the achievement. Finally, the removal or alteration of such a copyright notice can serve as an extra ground to pursue claims against a person which has taken material from one‘s own website (see sec. 2.1.5 below).

2.1.2 Ownership of Protected Content

As soon as the company establishing a website has decided on the material to be included on the website, it needs to identify the owners (i.e. rightholders) of the protected material it wants to use.

The European Member States‘ copyright laws grant the copyright in protected content (usually referred to as „protected work“) to the author of that work. The author is the natural person which has created the work. This means that a legal entity cannot be the original owner of a copyright, while it may – by a valid transfer of rights – become rightholder of certain rights of utilisation (usually referred to as „economic rights“) granted by copyright laws. In most EU countries, however, the copyright as a whole is not transferable to a third party, as only the „economic rights“ can be (and usually are) transferred. An exception can be found in the Irish Copyrights Acts and the UK Copyrights, Designs and Patents Act under which the creator of a work may transfer the copyright as a whole to another (natural or legal) person while the person who originally created a work will still be the initial rightholder.

An exception to these principles is the creation of a work in the course of an employment, under a service contract or in an apprenticeship. In these cases, most countries statutorily provide for a transfer of the rights of utilisation or (where possible, as in Ireland and the UK) the copyright as a whole from the author to the employer. Only the moral rights (see sec. 2.1.3 below) will remain with the work’s creator.

With regard to works created by several persons, all European copyright laws grant the copyright to the collaboration of authors in case the respective contributions cannot be separately exploited (otherwise each author holds the copyright to his contribution).

Within the area of EU harmonised copyright law (i.e. copyright protection for software and databases), generally the same principles as described above apply: Initial rightholder is the creator of the work, while the same exception applies to works created in the course of an employment – here the employer is the initial right holder of the economic rights. Again, only the economic rights can be transferred.

For databases protected by the related sui generis right (see above sec. 2.1.1), the rights are held by the maker of the database – that is the natural or legal person which has invested time, money or labour in producing the database. Here, the rights granted are all freely transferable.

→ As long as a company is not offering their own material only, a company which has identified the material it wishes to utilise for its internet presence needs to investigate who the current rightholder of the material in question is. For the majority of the protected content the essential economic rights have been transferred from the creator to either a company utilising the content or to a so called collection society which licenses the rights on behalf of authors. In some countries so called „multimedia clearing houses" provide for a „one-stop-shop" where interested parties can receive all the rights necessary for utilising material online.

TIP

They can be found online at:

Sesam (France): http://www.sesam.org/english/sesam/index.html

Clearingstelle Multimedia für Verwertungsgesellschaften von Urheber- und Leistungsschutzrechten GmbH, CMMV (Germany): http://www.cmmv.de/

Kopiosto (Finnland): http://www.kopiosto.fi/english/default.htm

Multimedia Copyright Clearance Ireland: http://www.mcci.ie/

Sociedad General de Autores y Editores (Spain): http://www.sgae.es/

Copy-Dan (Denmark): http://www.copydan.dk/index.asp?FE_ID=1&ML_ID=57

Società Italiana degli Autori ed Editori (Italy): http://www.siae.it/Site2/SiaeMainSite.nsf

CEDAR (Netherlands): http://www.cedar.nl/

2.1.3 Licensing Issues

After identifying the rightholders of the protected content the company now needs to know which rights it has to acquire in order to use the material online.

For copyright protected works the laws of the EU Member States provide for certain rights to utilise the work (so called economic rights) and further so called moral rights. For content protected by related rights, e.g. the sui generis right for databases, only economic rights are granted.

To a certain extend, the exclusive rights will be harmonized on a European level by the new Copyright Directive[3] the EU has recently adopted. Member States are obliged to implement the Directive before the 22nd of December 2002.

According to the new EU law, the relevant (transferable) economic rights in the online environment are the reproduction right (as the material needs to be uploaded on a server and sometimes initially be digitised which both involves an act of reproduction according to the relevant EU Directives) and the right of making (protected content) available to the public (as the possibility to retrieve the material from a freely accessible website involves its making available to the public according to the relevant new EU Copyright Directive). Apart from these rights the company, in case it plans to somehow alter or modify the material in any way, should get the permission from the rightholder and – in case it is a separate person – the author to do so.[4]

The moral rights granted to the author include the right to be recognised as the author and the right to prohibit distortion or other mutilation of the work. These rights cannot be transferred to third parties. Therefore the company should ask for an explicit statement/authorisation by the author that its intended utilisation does not interfere with the moral rights of the author and that he will not invoke any of his moral rights against the company for utilising the material in the agreed form. The company should further mention explicitly who created the work which is used on the webpage (thereby complying with the right of the author to be recognised as the author).

In order to acquire the necessary rights from the rightholder the company needs to negotiate a license agreement with the rightholder. As licensing in Europe is in some Member States bound to formal requirements, the license should be in writing and signed by both parties. There are no further formal requirements and thus the license can be an informal letter in which the rightholder is asked to transfer the necessary rights to the creator of the website.

[3] Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society.

[4] This is so because some national laws see the right to authorise alterations or modifications as part of the moral rights which cannot be transferred. Thus the company should try to seek a respective authorisation.

→ When drafting a license agreement with the rightholder/author, the company should:

- Include a preamble which describes the purpose of the license agreement (stating what the company plans to do with the licensed material);
- Include an exact description of the material licensed (addressing further the format, quality, etc. of the material) combined with an annex in which a copy of the material is included;
- In the rights transferring clause explicitly state:
  - What it technically needs to do with the licensed material (in order to use it the intended way),
  - how it economically plans to utilise the material,
  - the necessary rights (combined with a clause such as „the licensee therefore transfers all the rights (technically) necessary to achieve this purpose) and
  - that the intended utilisation of the licensed material does not infringe any of the moral rights granted to the author and therefore the author will not claim any moral rights violation based on the intended utilisation of the material;
- Further determine the duration of the license (any time limit at which the rights expire?);
- Exclude any geographical restrictions for the use of the material (as the company wants to use it online and thus world-wide),
- Include a clause whereby the licensor guarantees/warrants that he is the rightholder of the material in question and owns the rights necessary to fulfil the obligations arising from this license agreement;
- Include a so called „intellectual property indemnification clause“ whereby the licensor, in case the licensed material is found to infringe any third party rights (e.g. because the licensor is not the owner of the material in question) is obliged to indemnify and safeguard the company from and against claims which arise from the utilisation of the licensed material.

These are by far not all of the relevant terms and conditions to be included in such an agreement – the detailed wording and further terms depend on the concrete situation at hand, the law applicable to the contract and the bargaining power of the parties. So that specific legal advice is recommended.

2.1.4 Statutory Exemptions to Copyright Protection

Not every form of utilisation of a work requires the authorisation of the rightholder. A company using protected content in order to establish an internet presence may be able to rely on a statutory exemption from copyright or related rights protection, depending on the material used and the purpose and circumstances of the use. All EU Member States recognise a number of utilisation activities which are exempted from copyright protection. Among other issues, the recently adopted new EU Copyright Directive (see sec. 2.1.3) aims at harmonizing the statutory exemptions in the national laws in the member states (see Art. 5 of the Directive).

In the following, firstly, the most important general copyright exceptions in the national laws of the member states shall be introduced and, secondly, the main exceptions to be found in the new EU Directive which are applicable to the internet environment shall be introduced:
Although it is difficult to generalise the exception provisions, it can be assumed that all European countries provide for exemptions in the following categories:

1. Exception for Personal Use

Allowed is the making of single copies for private use, for personal scientific use or for personal information. The national jurisdictions decide differently on the question how many reproductions still fall under the term “single copies”. However, it will be safe to assume that two or three copies do not exceed the limit. Copies made under the exception for personal use may neither be distributed nor used for public communication, nor be made available on a homepage.

2. Exception for Educational Use

In similar manner, it is permissible to make copies in required quantities for teaching and examinations in schools, universities and other non-commercial institutions of education.

3. Quotation Exception

Quotations of various length in an own work are permissible if justified by the purpose of the quotation. This exemption includes not only the reproduction right but also the distribution right and communication to the public. Due to the author’s moral right to be recognised as the author, the author’s name and the citation’s source have to be mentioned in the work.

4. Reporting Exception

For the purpose of visual and sound reporting on events of the day, it is permitted to reproduce, distribute and communicate to the public works which become perceptible in the course of the reported events. In the same manner, speeches on questions of the day made at public meetings or in broadcasting may be reproduced, communicated to the public or be made available.

5. Conservation Exception

For the purpose of archiving material, most European copyright laws grant the right of reproduction to non-commercial facilities such as libraries, public educational facilities and the like.

These exceptions to copyright and related rights are granted by the national laws of the EU Member States. They may partly be influenced or changed by legislation implementing the new EU Copyright Directive. This Directive provides for a long list of – mostly optional – exceptions which among other things also address all the issues already regulated by national law (as described above). Therefore it can be assumed that the situation as regards copyright exceptions will not change considerably. Nevertheless, the most important exceptions as provided in the new EU Copyright Directive shall briefly be described:

1. Temporary Acts of Reproduction

Since the reproduction right as regulated by the new EU Directive in general covers any acts of reproduction, temporary reproductions of protected works have been explicitly excluded if they are incidental and a part of a technological process which purpose must be to enable

(1) a transmission in a network between third parties or

(2) lawful use of a work to be made.

Further these acts of reproduction may not have an independent economic significance as to the utilisation of the work. Typical acts covered by this exemption are proxy caching by Internet Service Providers or RAM copies made in the home computer of a private user.

The following exceptions deriving from the new EU Copyright Directive are optional for the Member States to implement – it thus remains to be seen whether and where they will continue to be or will become part of the national copyright laws of the Member States.

2. Reproductions for Private Use

Making (electronic or non-electronic) copies of a protected work does not infringe the reproduction right if these copies are made by a natural (in contrast to a legal) person for private and non-commercial use.

3. Reproductions and Making Available to the Public for Teaching and Research Purposes

Uses of protected material for the sole purpose of illustration for teaching or scientific research, as long as – if possible – the source (including the author's name) is indicated and to the extent justified by the non-commercial purpose to be achieved do not require the authorisation of the rightholder.

4. Reproductions and Making Available to the Public by the Press

Already published articles on current economic, political or religious topics or broadcast works or similar material, in cases where such use is not expressly reserved, and as long as the source (including the author's name) is indicated may be reproduced and/or made available to the public. Further the use of works or other protected material in connection with the reporting of current events, to the extent justified by the informatory purpose and as long as the source (including the author's name) is indicated does not require an authorisation.

5. Other Exceptions

Further exemptions to copyright and related rights cover the right to make quotations of protected material for purposes such as criticism or review, the use of political speeches as well as extracts of public lectures or similar works to the extent justified by the informatory purpose and the use of protected material for the purpose of caricature, parody or pastiche.

With regard to the copyright and related rights protection for computer programs (software) and databases harmonised by the respective EU Directives (compare sec. 2.1.1 above), different and generally more restrictive exceptions to the protection offered apply. Exceptions relating to computer programs such as the right to decompile or the right of the lawful user to make a back up copy are not specifically relevant in an internet context. Relevant exceptions to (copyright or sui generis) protected databases cover use of the database for teaching or research purposes. One has to be aware of the fact that – distinct from the general exceptions to copyright law as described above– none of the exceptions for computer programs or databases extend to making copies for private or personal use.

→ A Company planning to use other rightholder's protected content when establishing its website should – before negotiating a license agreement with the rightholder – check whether

its intended purpose to use the content might fall under one of the exception categories provided by copyright law. Insofar as this is the case, the company does not need a license to use the material in the way which is covered by the exception.

→ Companies should, on the other hand, be aware that their own material may also be used by others – especially users relying on the respective private use exception – without authorisation if this use falls within one of the exception categories.

2.1.5 Protection Against the Circumvention of Technological Measures and the Modification or Removal of Rights Management Information

The new EU Copyright Directive has introduced a new form of „indirect" copyright and related rights protection measures which have to be implemented in national law by the Member States until December 2002. The relevant provisions deal (1) with the protection of technological means such as anti-copying devices against circumvention and (2) with the protection of so called rights management information against removal or modifications.

With regard to technological measures which have to be designed to prevent or restrict unauthorised acts in relation to the protected material the act of circumvention and also the manufacture, import, distribution and sale of circumvention devices is prohibited. One has to add that regarding copyright protected computer programs (software) the import and distribution of devices aiming to circumvent technological protection measures is already prohibited due to earlier EU legislation.

Rights management information, defined as any data provided by the rightholders which identifies the protected material, the author or any other rightholder or any information about the terms and conditions of use of the protected material, are protected against removal and alteration or modification. Further, the import, distribution or making available to the public of protected material from which rights management information has been removed or modified is prohibited.

→ A company establishing an internet presence should be aware of this new forms of protection. It may provide for an incentive to use technological measures (such as access protection systems or anti-copying devices) to prevent unauthorised use of the companies protected content since the circumvention of such measures will soon be prohibited by law.

Companies should further start to make use of copyright notices mentioning at least the rightholder of the protected material. Apart from the advantages described in sec. 2.1.1 above such notices or other forms of right management information will soon be protected against removal or modifications.

→ On the other hand, the company should ensure that it does not remove or alter any copyright notices from the material it has acquired for its website without the consent of the rightholder to comply with the provision on rights management information.

2.2 Questions Related to Hyperlinking and Framing

Hyperlinks are a very useful element of the World Wide Web, both for users and for website owners. However, under certain conditions the usage of hyperlinks can be problematic for different specific legal reasons, e.g. trademark law, copyright law, competition law or liability reasons.

2.2.1 General Liability Aspects

One issue which is relevant when designing a website is the question of whether someone who links to another website can be held liable for the content of the website to which he has set the link.

2.2.2 Trademark Aspects of Hyperlinking

Often protected signs such as trademarked names or logos are used - to some extent almost have to be used - within the design of a hyperlink. Many hyperlinks are designed in such way that a certain word or words on a website is written in ordinary characters and is in some way emphasised, e.g. underlined, appearing in a different colour than the rest of the text, which can then be clicked at to follow the link. Even in these “basic” links the words which can be clicked will often consist of protected signs, trademarks or trade names of the company to which is being linked. Each basic hyperlink on a commercial site in which a protected trademark is used would therefore represent use of the sign which could constitute an infringement if not permitted by the owner of the sign. The use of hypertext is however a predominant characteristic of the Internet and usually a person will be in favour of links to his website as this increases the number of visitors on the site and its success. It is generally

argued that the act of putting a webpage on the Internet contains an implicit consent to the setting of regular hyperlinks to the *homepage* of a website (so called „surface links“).

It can however not be said that any form of hyperlinking does not require an explicit agreement of the rightholder. The use of protected logos in icons which are hyperlinked is not covered by the implicit consent.

Even the use of a “basic” hyperlink can in some cases constitute an infringement. This is usually relevant only in relation to the use of well-known trademarks. Two different situations may occur in this respect. If the name is used on a website which is incompatible to the reputation of the trademark (e.g. a Disney trademark on a pornographic website), the reputation of the well-known trademark may be effected, which constitutes an infringement of the protected sign. Even of greater importance are situations in which well-known trademarks are used in “virtual malls”, in “link lists” which are commercially exploited e.g. by advertising banners. Such integration of well-known trademarks may be regarded as exploiting the reputation of the sign and therefore also as constituting an infringement.

→ Companies wishing to set hyperlinks on their commercial sites to websites of (famous) brands should inform the rightholder about this and ask for their agreement to set the hyperlink as this is the easiest way to avoid later conflicts. Also in case a company would like to use a protected logo, name or sign as an icon to hyperlink to a third party’s website it is recommended to ask for prior permission for the link in this design.

→ With regard to hyperlinks pointing to one‘s own website it should be considered to include a clause in the licensing conditions on one‘s website determining under which conditions hyperlinks may be set and whether logos etc. may be used for such links.

2.2.3 Copyright Aspects of Hyperlinking

Normal hyperlinks to the *homepage* of a website (surface links) are not considered to be an infringement of copyrights and related rights as the linking person does not copy the targeted content nor make it available to the public in a legal sense and therefore does not infringe the author's reproduction right but rather shows where a certain content is to be found. There are,

however, cases in which the further circumstances of hyperlinking (especially the web page to which the link directs a user or whether and how the hyperlink integrates the linked content into the linking page) may result in copyright or related rights infringement by the person setting the hyperlink.

If a hyperlink does not target the homepage but another, secondary page (so-called deep link), the advertising on the homepage is by-passed by the user. This is problematic as the owner of the site has fewer hits and possibly less advertising income. Furthermore, it is the homepage where the company or organisation is presented, and, finally, disclaimers and conditions on the use of the material are usually to be found there.

If the targeted site is put into a frame of the linking site (framing), the linked site seems to be part of the linking site. As a result, the user might believe that there is at least a relationship or co-operation between both sites.

Finally, a part of the targeted site, especially an image, can be integrated into the linking site itself (so-called inline links). By using this kind of link the owner of the linking site saves server space and the image – although stored on the server of the linked website – appears as part of the linking site. Since the URL of the integrated picture is not indicated, the user is not aware of its origin.

The above kinds of links might amount to a copyright infringement or to an act of unfair competition. Until today, it is not sure whether courts will consider deep links as an act that has to be authorised by the rightholder of copyright or related rights protected content. Because of the above-mentioned importance of the homepage for the site owner, the establishment of a deep link can cause an important damage for the owner of the concerned site. In addition to this damaging effect, the linking site takes unfair advantage of the work the owner of the concerned page has invested. Therefore, unauthorised deep links could be deemed to be an act of unfair competition.
As regards framing, the moral rights (see above sec 2.1.3) of the authors of the framed site may be infringed. If the targeted content is placed into a different context, e.g. into the frame of a pornographic site, or if only a part of it is put into the frame, the author’s right with

respect to the integrity of his work might be violated. Since the framed content appears as part of the framing site, framing also may infringe the author's right to be recognised as such. For the same reason framing amounts, in many cases, to an act of unfair competition or to passing off.

However, since especially deep links and even frames are very frequently used kinds of links and as they offer also important advantages to both website owners and users, the courts might also decide that every website owner has implicitly given his agreement, by the mere presence on the Internet, to deep links to his site or to the framing of his pages.

Inline links will, in most cases, amount to a copyright infringement (if the link integrates copyright protected content in the linking website) or to an act of unfair competition unless the right-owner of the targeted site has given his consent. It cannot be assumed that the right-holder has implicitly agreed to this extreme kind of linking.

→ A company which has established an internet presence should make clear in a copyright remark on its website which kind of link to the site it agrees with. If one wants to avoid deep links to his secondary web pages, one should include the following notice: "Link to this page only by using this address: http://www.example.com" or "Please direct your link toward the homepage only. Use the following text as hyperlink information: ...". The company should also consider technological solutions against deep-linking.

→ If a company wants to avoid that its webpages are put into a frame, it should include the following notice on its pages: "Please do not frame this page." These notices might also be useful when the company sues the owner of the linking site for damages and it has to prove that the infringement of intellectual property has been caused by negligent conduct or happened wilfully. Further, with a notice as described above in relation to the webpage which should not be linked or framed, no one can argue in front of a court that he has relied on a implicit authorisation to link/frame to its page. However, one should bear in mind that these kind of notices do not have the same legal value as a binding contract between the linker and the operator of the linked page. If courts hold that deep linking or framing of one's site does

neither infringe copyright nor amount to an act of unfair competition, the notices are without any legal value since they then cannot make the act of linking or framing infringing.

→ With regard to inline links, a company having established an internet presence should include in its copyright notice (see above sec. 2.1.1 and 2.1.5) a sentence such as: „Inline links to any of the protected content of this website are a violation of international copyright laws and not tolerated by the website owner".

→ On the other hand again, a company should ask the owner of the targeted site for his permission if it wants to create a deep link, a frame or especially an inline-link to material which is hosted on a third party website. It is also advisable to make sure that the web site owner or operator is legally in the position to grant the necessary license.

TIP

Useful information on the topic of linking can be found on Stefan Bechthold's The Link Controversy Webpage- both information on technology and linking agreements can be found there, see http://www.jura.uni-tuebingen.de/~s-bes1/lcp.html#licenses

2.3 Search Engine Related Issues

A number of disputes have recently arisen in relation to the functioning of search engines which continue to gain importance for using the internet.

2.3.1 The Use of Meta-Tags

One aspect is the use of trademarks or otherwise protected names, logos or signs in meta-tags. Meta-tags are keywords which are inserted in the source code of a website and which are not visible for an internet user on the actual site. If someone searches for a certain keyword using a search engine, the search engine will also list the website which only contains the term in a meta-tag. Some companies therefore use trademarks of their competitors in meta-tags on their pages to the effect that a search engine will list their website whenever someone executes a search for the competitor's trademark. If such meta-tags are cleverly used, the company which uses a third party's identifier in its meta-text will even be listed at a better position than the website of the rightholder.

The trademark holder certainly has an interest to stop such use of his trademark in meta-tags. In several cases courts have held that the use of a third party's sign in meta-tags constitutes a trademark infringement. Decisions have also been based on unfair competition law, saying e.g. that the indication of the competitor's website is misleading and deceptive. Only in cases in which the user of the meta-tag has a right to use the term in relation to its business, the use of the sign is allowed.

Although courts and legal experts do not completely agree whether and which trademark infringement option or unfair competition case category is given in cases of abusive meta-tagging, there appears to be a common understanding that such business practice is to be prohibited.

→ It is strongly recommended to refrain from illegitimate practices of meta-tagging. Only generic terms or distinctive signs which are used with the consent of the rightholder should be used in meta-tags.

→ In order to protect one's own rights, a regular search engine watch is recommended. By effecting a search for ones own trademark/trade name, undesired search results can easily be found. Abusive meta-tagging can then be detected by looking in the source code of the website which the search engine wrongly refers to. If a company realises that a competitor is using its trademark or trade name within his source code, a local lawyer should be consulted which knows the state of jurisdiction with regard to these matters in the concrete country.

2.3.2 Keyword Selling

Certain providers offer a new form of use of a third party's trademark with regard to search engines. Certain keywords can be "bought" to the effect that whenever a person effects a search for such keyword an advertisement banner of the keyword-owner appears on top of the page which lists the search results. If such a keyword is identical or closely similar to a well-

known trademark it is likely that courts will qualify this proceeding as taking undue advantage of the distinctive character or repute of the trademark.
For determining the degree of fame not the general public but only the interested sections of the population are taken into account. Claims based on competition law may be successful as well as claims for taking undue advantage of a third party's goodwill.

→ Although it cannot definitely be predicted how courts will judge the practice of keyword selling it is recommended to sustain from "buying" a competitors trademark or trade name. Only generic terms or terms to which oneself holds a right should be used.

→ If a company finds out that a competitor has bought the company's well-known trademark as a keyword, it is advisable to contact legal advise in order to protect one's trademark against such most probably infringing use

TIP

The WIPO Arbitration and Mediation Center offers a specialised alternative dispute resolution procedure for keyword disputes, see http://arbiter.wipo.int/keywords/index.html

2.4 Remedies in Case of an IP Rights Infringement

If any of the economic or moral rights that have been addressed in this chapter are infringed, the copyright legislation's of the European countries provide for civil and criminal remedies. Civil remedies include actions for injunctions and damages, a claim to destroy or surrender unlawful copies or devices used to manufacture unlawful copies, and the right to obtain information as to the origin and distribution channels of unlawful copies, if the copies have been manufactured or distributed in the infringing parties' course of business. Criminal remedies vary from country to country (usually starting with a fine and ending with a term of imprisonment of up to five years) and depend on the infringing act.
When a company decides to take legal measures in order to seek remedies for an alleged infringement of its intellectual property rights, it is faced with the task to determine the correct place of jurisdiction. Similar to its effect on the questions of applicable law (see above sec. 2.1.1), the inherent international nature of the internet challenges the rules of international civil procedure law, which governs questions of jurisdiction in controversies with an

international character. This results in complex new problems which are beyond the scope of this brochure. Therefore detailed legal advice is required in each individual case.

As a general rule with respect to EU member states, however, a provision of the Brussels Convention[5] governing jurisdiction in tort cases is applicable to IP infringement issues. It establishes jurisdiction both in the country where the allegedly infringing act was committed and in the country where the injury arose (in case of alleged IP infringements, wherever rights granted to the rightholder are potentially violated), leaving the plaintiff with a choice: As protected content placed on a website is accessible in each of the member states, the plaintiff may take legal action in the country in which the alleged infringer operates his websites. But he may also choose any other (European) jurisdiction, as IP rights are potentially infringed wherever the content is accessible to internet users, since the unauthorized act of making IP protected content available to the public will constitute an infringement under the new European Copyright Directive (see sec. 2.1.3 above)

While this possible choice of jurisdiction may obviously benefit a company as long as it tries to protect its own content in the online world, it may, on the other hand, be fatal if the company itself infringes someone else's copyright, as the company may find itself faced with claims for injunctions or damages in any one of the member states.

This possible result of an IP right infringement once again underlines and stresses the enormous importance of being aware of the numerous Intellectual Property issues addressed in the above chapter when designing and running a website.

[5] Brussels Convention on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, which applie to all member states.

APPENDIX

GENERAL CHECKLIST FOR DESIGNING AND BUILDING A WEBSITE

CONTRACT WITH THE WEBSITE DESIGNER

The following points should be kept in mind:

- **Existing rights:** make sure that the material (pictures, graphics, etc) and in particular the software tools (e.g. shopping basket software) are properly licensed and do not infringe third party rights.

- **Ownership of copyrights and other intellectual property rights:** make sure you are aware of who owns what. Who provided the text, logos, graphics, pictures, music, the overall design and the software? The creator is usually the owner of the copyright in these items- you should pay particular attention to any necessary transfers.

- **Bespoke Software:** if the designer specially develops bespoke software tools for your website make sure that the intellectual property rights are transferred to you expressly. If this is not done the supplier will retain copyright. Be aware that you might need specific legal advice for a contract for the supply of bespoke software.

- **Charges for Updating and Maintenance:** Charges are usually either based on the hours spent or the number of pages. However a few quick changes or changes to detail should be made free or for a small flat rate. The services covered under the maintenance contract should be clearly detailed including response times.

- **Deadlines:** It will be advisable to set out a clear timetable with deadlines for the production of the initial proposal, specifications, the alpha version, beta version and live version. You should specifically provide who has to supply what and by what date.

INTELLECTUAL PROPERTY ON WEBSITES

- **Infringement:** If you intend to use third party material, check whether this is copyright protected or whether any relevant trademarks have been registered. Also be aware that the website can be accessed from anywhere in the world so that infringement can occur in any country. To be safe make sure you get written permission to use the material on your website.

- **Protection of your material:** Copyright protected material includes text, logos, graphics, pictures, music and sounds. Copyright arises automatically, so that strictly speaking you are protected even without a formal notice. However it is advisable to include a notice in the correct form © John Blokes 2001, as this creates a legal presumption in your favour and might help in any dispute. Make sure you register any trademarks in the relevant jurisdictions. A registered trademark is indicated by the ® sign after the mark.

- **Linking:** It is not clear whether linking to another homepage is not an infringement of copyright, whereas linking to a site beyond the homepage (deep-linking) and framing are probably illegal. In any case this is a complex area of law and therefore it is advisable to obtain the express and written permission of the owner of a website before linking to it.

  It would be advisable to include a statement on your website whether or not you allow other websites to link to your site and under which terms. You might wish to ensure that advertising revenue is not lost by users linking to a deeper site or you may be concerned that you or your content is not associated with other sites. On the other hand linking may lead to an increase in traffic.

Make sure there are specific clauses covering set-up, service levels, downtime and response time. There should be clauses covering maintenance and back ups, providing for a disaster recovery plan. Usually the ISP will only give you a "best endeavours" guarantee, i.e. that it will do everything reasonable to provide uninterrupted service and that it will repair faults quickly.

T SERVICE

HOSTING AND ACCESS AGREEMENTS

LEGAL CONSIDERATIONS

Your business may suffer serious disruption if your website is down or where you cannot receive and send e-mails. This checklist is to consider some of the main clauses to look out for.

Make sure that that the contract contains specific clauses providing for security (e.g. against hacking and viruses). Furthermore the contract should deal with liability for loss of data. Also the ISP should be under an express duty of confidentiality.

Make sure there are clear obligations on the ISP provider for those aspects of the service which are under its control. The ISP should guarantee the availability of support staff when needed. Furthermore the contract should require it to provide regular reports about the availability and speed of the service.

Termination provision: make sure that the ISP cannot terminate the agreement at short notice.

Be aware that the ISP will wish to impose a guarantee that the material on the site is lawful and liability if it is not. The ISP will probably want to include a clause that it is entitled to take down illegal material. Make sure that these clauses are not worded to widely...

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 3

Designing the Web-contracting Process

CHAPTER 3

3. Designing the Web-contracting Process

3.1 Introduction

The technical conditions of Internet and Electronic commerce challenge contract law in a special way and put forward a number of questions inevitably in this area.

This part of the brochure deals with the “procedural” issues of contract law, that is, how a contract is concluded and what its contents are. The contract contents are partly mastered by consumer protection regulations. Therefore the appropriate consumer protection rights are already treated under this chapter in brevity.

The further “substantive” rights conceded to consumers when they contract electronically are a matter explained in chapter on consumer protection.

The main aspects of contract law are governed by national laws. Beyond any international differences, one common characteristic of national contract law regulations is their relative uncertainty and hence flexibility, as contract law everywhere is built on such vague concepts as consent, consideration, good faith, reasonableness, etc. There are generally no specific national regulations for electronic contracts.

Without unification cross-border contractual relations will be impaired by these uncertainties. Thus, one party may consider, on the basis of her own legal system, that no contract has been concluded, while the other party may come to the contrary solution on the basis of her legal system.

The European Commission regards electronic commerce as a unique opportunity for economic growth. Therefore there are many regulations at the European level. Material interventions in the national legal provisions have to be expected from the Directive on Electronic Commerce. This has become effective as Directive 2000/31/EC on June 8th, 2000. It provides a framework, which only addresses the most important questions. It leaves space for the parties involved for self-regulation. The Member States shall transpose the Directive before 17 January 2002.

Even though the rules of international private law almost ensure that the laws of the supplier's nation will govern the contracts made on his e-commerce platform, a merchant who wishes to gain the confidence of a wider, European market must adopt a "European best" attitude when building or selecting an e-commerce platform. That means that this platform must match what any purchaser may expect according to his national perspective.

Thus the merchant's platform must fulfil the highest legal requirements in Europe.
This "legal best" approach is assumed in this paper and guides the drawing up of all the recommendations included in it.

3.2 Conclusion of Electronic Contracts

In principle a contract can be completed via Internet like in normal offline business. In principle the conclusion of a contract does not require any particular form. A contract may be effective whether concluded verbally or by e-mail or on a website. Professed intentions can therefore for example be given by sending e-mails or by filling out ordering forms and sending over the Internet.

The contact between supplier and customer takes place by the fact that the customer visits the web pages of the supplier in the Internet. Here, the supplier presents to the customer different products in the context of an E- Catalogue. In this place the question arises, of whom and at which time the supply- and by whom the declaration of acceptance is handed in.

3.2.1 Presentation the E- Catalogue

Generally, the offering of the products or the service on a website is only an invitation to treat and not the expression with the intention that they will become legally binding on acceptance by the addressee.Otherwise, the shopkeeper or advertiser might be bound by many more contracts than he has goods in his stock, making himself liable for compensation. The EU Directive on E-commerce also is based on this position because there is the talk of an order by the user. Nevertheless, companies are advised to indicate and express this on their web site to obviate uncertainties. But in the end this question depends on how the website is designed.

3.2.2 The Legal Offer

Therefore, the visitor of the web site will make the first legal offer by completing the order form and its subsequent transmission to the company.

About the order of the customer as an offer with the intention to create legal relations the Content provider decides in a liberal estimation whether he accepts the offer. What conduct constitutes a binding order by the customer? As a rule, it does not lie in the choice of a product by mouse click and the admission to the list of the objects selected by him yet ("shopping basket" "trolley"). What lies in the "trolley", the customer can regularly take out again. Here, the supplier should provide that the admission of a product to the list is not binding. The consumer is bound on confirming the order.

Furthermore the EU Directive on E-commerce states that the customer must be given an opportunity to correct any input errors. Also he must inform the user about it. Today, confirmation buttons are already used which the customers show the content of their electronic order once again and give them the chance for a correction. In this respect it is simply to manage the measure technically.

3.2.3 The Acknowledgement of Receipt

The Directive on Electronic Commerce states, the supplier is "obliged to immediately send the acknowledgement of receipt" at the end of the process. Checking the stocks should be done before purchaser acceptance (the second click). The acknowledgement of receipt may serve only to confirm that the acceptance click has been received by the supplier. The acknowledgement must be sent within the time strictly needed to provide such a confirmation of the reception, which may be a few seconds when we are operating on a Web contracting platform.

3.2.4 The Legal Acceptance

If the customer has ordered a service which can be rendered online, for example software or the access to a data base for a fee, the acceptance is the conclusive behaviour of the supplier, namely by conduct of the performance. Here, the entrance of the declaration of acceptance with the customer is dispensable just like in the mail order business.

Under article 6 of the Directive on distance contract a final consumer has the possibility to revoke the completion of a contract within at least seven working days or at missing instruction within three months.

Tips for the Construction of a Web-site:

The First Click

- **One Click is Not Enough**

  It must be assumed that e-commerce's usual platform, where consent is expressed by clicking, dragging, or similar actions, lacks "contractual expressiveness". The complexity of the technological tools used to conclude contracts (computer complexity plus Internet complexity) and the non-negligible possibility of inadvertent clicking to diminish the "expressiveness" of the purchaser's actions on the e-commerce platform.

Consequently a two-click (at least) process must be built up in e-commerce platforms, both to ensure that the parties give their full and informed consent and to permit the detection and correction of handling errors.

- **Informing of the Non-Binding Nature of the First Click**

  The non-binding nature of the first click should be clearly indicated to the potential purchaser. The “shopping cart”, “shopping bag” or similar presentations are expressive enough of this aspect.

The Recapitulative Page

- **Products**

  The recapitulative page must contain a summary of the products to be purchased. A minimal description of each is needed in order to allow purchasers to detect their errors. If only a code-number or similar designation, for example, is shown, this is not fulfilled. Weight, colour and other characteristics of the product that have been selected by the purchaser should also be shown.

- **Product Prices**

  The price of each product to be purchased and the total cost of the purchase should be shown.

- **Transport Prices**

  If the recapitulative page contains the last opportunity for the purchaser not to close the contract, transport prices should be shown here. They may be shown only once (on this page), as they are not affected by the two-click process, which is needed only for the core of the contract.

- **Cancellation and Correction Opportunities**

  Buttons or similar devices should be offered to permit the cancellation of the total purchase or of one or more products. An opportunity to correct the quantity of items or their selected characteristics (weight, colour, etc.) should also be given.

The Second Click

- **Clear Meaning**

  The button where the second and final click is made should clearly explain its meaning. Words like order, buy, or pay seem expressive enough to need no other information.

- **Time between First and Second Clicks**

  A reasonable time may pass between the first click and the second, as there is no reason to require that they be produced in rapid succession. Unless intelligent agents are used this may allow the supplier to process the order and check stocks before becoming contractually bound.

3.3 The Content of the Contract

The European legislation imposes duties on suppliers to provide information. Further indications for this topic are given under the chapter of consumer protection and in the summary below.

1.9.1.1 3.3.1 Advertisement and Contractual Content

Furthermore the contractual content still is determined by other factors. The content of the contract (and therefore what each contractor may expect and demand from the other) is formed according to two different rules. The first is the “consent” rule, which adapted to e-commerce means that everything that, in the broad sense we will see below, has been accepted by the purchaser obliges both contractors. The second is the “advertisement” rule, which means that everything that could have influenced the purchaser to conclude this contract but cannot be considered as accepted by him may be demanded by the purchaser (and not by the supplier) except if this advantage is expressly excluded in the contract. Thus it can be said that the content of advertisement joins the content of the contract if the contract omits all reference to it. This rule finds its widest application when consumers are affected and, as we will see, can absolutely not be underestimated by participants in e-commerce.

3.3.2 Product Quality and Performance

Rules about the standards for purchased products, although very similar, present some differences among European national laws. We therefore took Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees as the base for the recommendations that follow.

According to art. 2 of this directive, and extracting what is most relevant for the purposes of e-commerce, the model that must be used to check if a given purchased product meets standards comprises:

- "the description given by the seller";
- "the purposes for which goods of the same type are normally used", and exceptionally "any particular purpose for which the consumer requires them and which he made known to the seller at the time of conclusion of the contract and which the seller has accepted";
- "the quality and performance which are normal in goods of the same type and which the consumer can reasonably expect, given the nature of the goods and taking into account any public statements on the specific characteristics of the goods made about them by the seller, the producer or his representative, particularly in advertising or on labelling".

Tips for the Construction of a Web-site:

How to Present the Description of Goods?

- **Descriptions in the Right Place**

The descriptions of the good that will be assumed to define standards are exclusively those placed on a mandatory page in the e-commerce contracting process (that is, a page through which the purchaser must pass) and those that are on a page linked to a mandatory page through a unequivocal, clear button or similar device. The e-catalogue page or pages is the

best place for this information. Neither the recapitulative page nor the page containing the acknowledgement of receipt is appropriate.

- **Descriptions Not in the Right Place**

According to the "advertising rule" any description not in the right place could be deemed not incorporated into the contract but serving exclusively the allegations of the purchaser.

- **Under-Average Quality**

Under-average features or quality (taking account of the price) must be transparently shown. For that purpose, the mere mention on a page linked to the mandatory page containing the e-catalogue does not fulfil what is required by the good faith and consumer protection principles, except when the description of the product in the e-catalogue is so brief as to ensure that any purchaser should have gone to the linked page containing the full description and this under-average quality is adequately emphasized there.

- **For What Purposes must the Product Be Fit?**

The meaning of "normal use", which serves to define for what purpose the purchased product must be fit, causes some difficulties in e-commerce, as its abstract nature raises the question of what "normal use" should be employed as the standard: what is normal in the seller's country or what is normal in the buyer's? As in traditional commerce, normality in the seller's country could be the surer solution, except when the consumer's expectation is produced otherwise, as would occur, for example, if the e-supplier's address is not shown on the e-commerce platform, the language of the buyer is used, or advertisement is made in national portals of the buyer's country.

- **What Can a Consumer Reasonably Expect?**

The interaction of traditional commerce allows buyers to ask easily and immediately for the information they need to check whether a product is suited to their purposes (and particularly whether it is compatible with their other possessions). The lack of this immediate interaction in e-commerce should be offset by the delivery of a large amount of information, in such a manner that a purchaser who does not find information about certain inadvisable uses or incompatibilities of a product may reasonably expect that it is valid for any use and compatible with any other product.

3.4 General Terms

European regulations on general conditions deal with two different matters: what conditions are unfair and thus void (content control), and what requirements must be met to ensure that the terms are included in the contract (inclusion control).

While content control rules are highly uniform in Europe, as a consequence of the Directive on Unfair Contract Terms, only certain countries (for example, Germany, Spain, France, Italy, Portugal) have specific inclusion control rules, although in other countries caselaw has established similar standards.

Inclusion Control

Tips for the Construction of a Web-site:

How to Include Ordinary General Terms in an E-Commerce Platform?

National laws regulating the inclusion of general terms currently require that these be made available to purchasers at the time of concluding the contract.

- **Direct Availability**

The general conditions should be directly available to the customer making the electronic purchase; a notice saying, “If you wish to know our general conditions send an e-mail to …” is not satisfactory.

- **Where to Place General Terms?**

    - **On a Mandatory Page**

General terms should be placed on a mandatory page within the contractual process. Taking into account the possibility of skipping the homepage by bookmaking or by access from external links or search engines, it is not an appropriate site to place the general terms. In our opinion, the e-catalogue and the recapitulative pages are the most recommendable places. Of course the page containing the acknowledgement of receipt, as defined in the proposed directive on electronic commerce, is not appropriate, because the general conditions should be available when forming the decision to contract.

- **Directly on this Page or Linked to It**

General terms may be placed directly on one of the mandatory pages or on another page linked to one of them. In this case, the link to the page containing the general conditions should clearly refer to them; phrases such as "More about …" are not clear enough.

- **General Terms Not in the Right Place**

What about general terms, contractual rules and features that are not in the right place? In our opinion, the "advertising rule" should apply, as these pages may have influenced the will of the consumer, though there is no certainty of that. Consumers may then demand features and clauses they are interested in, but may decline them if they are not to their advantage.

- **How to Present General Terms?**

Since the general conditions should be clear and comprehensible, the use of fancy pages with excessive graphics, java and links is not satisfactory for the link or for the page containing the general terms.
The presentation of the general terms may be done on scrolling pages or in a hierarchical mode, but avoiding really user-unfriendly presentations.

- **How to Include Extraordinary General Terms?**

A typical rule of inclusion control regulations consists in the prohibition of surprising clauses. Taking advantage of careless acceptance of general terms to slip in unexpected and right restricting clauses is usually considered to be not complying with the due good faith.

Exceptionally, national regulations allow clauses of this kind if they are either separately signed or at least detached enough: this is the “red hand” rule.

- **How to Detach Them?**

It is not enough to underline these clauses on the page containing the general terms if this is a page linked only to the principal pages in the contracting process. Onerous clauses must be clearly pointed out.

- **How to Accept Them?**

If national laws require not only detachment of the clauses but also their separate signing, a specific accept button should be added to what we have said before. Mandatory conditioning access to the last page (in the minimal process, the recapitulative page) upon clicking the accept button is, in our opinion, complying with this rule.

3.5 The Evidence

Since contracts that are entered into electronically can be changed afterwards there may be problems to prove the terms of the contract.

There is an EU Directive on Electronic Signatures ensuring that electronic signatures are recognised throughout the EU, if a certificate and the service provider as well as the signature product used meet a set of specific requirements. Moreover, they can be used as evidence in legal proceedings.

Also, under the Directive on Electronic Commerce the member states have to make, possible the conclusions of electronic contracts. The fact that a contract has taken place on an electronic way shall not be allowed to lead to the invalidity or ineffectiveness of the contract. After this every electronic text fulfils in writing independently how it has taken place.

3.5.1 Evidence of the Existence of a Contract

Evidence of the existence of an electronic contract may be produced by a digitally signed acceptance. Such contract may also been shown by actions of the acceptant, such as making or ordering payment or accepting delivery of the purchased products.

3.5.2 Evidence of the Content of a Contract

Because exhibiting an e-commerce platform, does not establish that this particular version of the platform was used to conclude the contract whose content is under discussion, if an e-supplier considers this lack of evidence a relevant risk, it could be recommendable to permit a third party (a notary or the like) to periodically check whether the e-commerce platform that is functioning is the one previously set up by the e-supplier.

Tips for the Construction of the Web-site:

The steps an e-supplier must follow before launching his e-commerce platform are the following:

1. Determining whether the contracts he wishes to conclude electronically are subject to any formal requirement under the applicable national law. If there is no such statement, the silence of the law must be interpreted as acceptance of electronic contracts.
2. Looking at the consequences of non-fulfilment of the formal requirements. If there are administrative or similar consequences (fines, non-acceptance in a registry, etc.) these should be previously considered. If the consequences are only that the contract is invalid and consequently not accepted in court.
3. Taking a decision based on a legal and economic analysis of considerations such as these:
    - The risk of the other party's rejecting the contract before it is performed or just when the purchased goods are to be delivered is similar to the risk existing in contracts lacking evidence and very similar -differing only in the payment of the cost of returning the goods- to the risk existing in contracts concluded with consumers (as they have a right of withdrawal).

- The risk of the other party's rejecting the contract after its performance (and particularly when payment has been made) is currently low, as he probably has to face presenting a judicial demand and he may not be sure that the court decision will bring whole restitution. Moreover, this risk (unlike the first) may be avoided by allowing the formalities to be fulfilled by delivery of the purchased products.

3.6 Issues of Private International Law

When contracts have links to more than one legal system, it must be decided which law is applicable and which court has jurisdiction to hear disputes that might arise. These are questions of Private International Law, and should be dealt with already in the contracting process.

Deciding applicable law and jurisdiction raises complex questions, and it would fall outside the scope of this brochure to deal with them in full depth. The objective of this section is therefore to give an overview of some of the most important problems that tend to arise, and what the parties can do to avoid them when entering the contract. However, it is recommended that more detailed legal advice is sought in each individual case.

The rules of private international are in principle a part of the domestic legal system of each state. However, many of these rules have been harmonised at a European level through international conventions. This brochure will only deal with these conventions.

3.6.1 Choice of Law

This section is based on the provisions of the *1980 Rome Convention on the Law Applicable to Contractual Obligations*. The Rome Convention governs the choice of law relating to certain contracts for the sale of goods or services within the European Union.

The first choice of law issue that must be decided is the relevant law for determining the validity of the contract. Article 9 of the EC Directive on electronic commerce[6] requires the member states to ensure there are no legal requirements in their domestic legal systems that create obstacles for the use of electronic contracts, or deprives contracts that have been made electronically of any legal effects. This means that contracts concluded electronically will normally be valid under the laws of all the EU and EEA member states.[7] Still, there might be certain differences in the legal requirements for electronic contracts to be valid under the different legal systems of the European states. For instance, there might be diverging requirements relating to the contracting process. It is therefore necessary to determine the applicable law. In accordance with the Rome Convention, the main rule is that the formal and material validity of the contract is determined in accordance with the laws of the country that would govern the contract had it been valid.

When determining which law governs the contract, the main rule is the principle of party autonomy. This implies that the parties are free to make an agreement as to which law is applicable, and the applicable law will normally be determined in accordance with this agreement.

If the parties have made no choice of law, the applicable law will be determined in accordance with the general provisions of the Rome Convention. In that case, article 4 of the Convention stipulates that the law of the county with which it is most closely connected governs the contract. This rule leads to a rather uncertain outcome, as each contract must be evaluated individually.

For these reasons it is strongly advisable that the parties agree upon which country's law is applicable to their contact. They can do this by including a choice of law clause in their contract. This will greatly reduce any legal uncertainty. However, it is important and advisable that the choice of law clause is sufficiently clear and unambiguous, and it should therefore be carefully drafted.

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

[7] The EEA member states consist of the EU members and Norway, Iceland and Lichtenstein.

The freedom of the parties to make a binding choice of law agreement is subject to certain limitations. These will typically apply when there is a qualified degree of difference between the parties in terms of negotiating strength, or where the link to a particular legal system is especially strong. Some examples are contracts for the sale of goods on instalment credit terms, and contracts of individual employment.

One of the most important restrictions applies to consumer contracts. The consumer cannot make a binding choice of law agreement that deprives him of any protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence. Also, in the absence of a choice, the law of the country where the consumer is resident will normally govern a consumer contract. The result is that the law of the consumer's home country governs most consumer contracts. For businesses that are selling goods or services to consumers on a European level this means that they will have to comply with consumer protection laws in several countries. This represents an extra burden for the business even if consumer protection legislation is harmonised to a certain extent within the European Union and the EEA. It is therefore necessary for the business to decide if they are willing to do this. If the answer is no, they could somehow try to limit their business to consumers from certain countries.

3.6.2 Jurisdiction

The rules described in this section are based on the provisions of the *1968 Brussels Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters* and the *1988 Lugano Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters.* These Conventions address jurisdictional and enforcement issues within the European Union and some other European countries. The Brussels Convention will be replaced by the *Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.* This regulation is largely identical to the Brussels Convention, and enters into force on 1 March 2002

If a dispute arises between the contracting parties it must be determined which country's courts have jurisdiction to hear the case. Again, in both Conventions and the new Council Regulation, the main rule is the principle of party autonomy. This means that the parties are normally free to make a binding agreement on jurisdiction. The agreement can be made either before or after a dispute has arisen, but it is often easier to reach an agreement beforehand. Therefore, it is strongly recommended that the parties include a jurisdiction clause in their contract, and that this clause is drafted clearly and unambiguously.

The choice of jurisdiction is closely related to the question of using alternative dispute resolution (ADR) services to settle disputes. These two questions should be considered in connection with one another, and in both cases the parties enjoy a great freedom of choice. ADR services are described in chapter 8 of this brochure.

If no choice of jurisdiction has been made, the general rule in the Brussels and Lugano Conventions is that the defendant shall be sued in the state where he is domiciled. Alternatively, article 5 of the conventions stipulates that the defendant party to a contract may be sued in the courts for the place of performance of the obligation in question. In consumer contracts, the consumer can also sue in the courts of the state where he is himself domiciled. This is also the only place where he can be sued himself. There are also other provisions that govern the choice of jurisdiction. In many cases it can be difficult to determine which court has jurisdiction in the absence of a jurisdiction clause.

The parties' freedom to choose jurisdiction is subject to certain limitations. Some examples are cases relating to immovable property, and matters relating to insurance. Another example is consumer disputes. The consumer cannot, prior to the moment that the dispute has arisen, enter into any binding agreement that deprives him of his right to bring proceedings before the courts that would otherwise have jurisdiction. Such agreements would not bind the consumer. This means that businesses dealing with consumers run the risk of being sued in several countries. If they which to avoid this, they could try to limit their business to consumers from certain countries.

3.6.3 Which Law and Jurisdiction Should the Parties Choose?

Before a choice is made, it must be determined if the parties' freedom of choice is subject to any restrictions. If so, these restrictions must be respected. However, to the extent that they are free to make a choice, the parties need to face the question of what the choice of applicable law and jurisdiction should be. There are several factors to take into consideration.

The choice of applicable law and jurisdiction is often subject to negotiations between the contracting parties. The parties can then reach a result that is acceptable for everyone involved. However, it is also common that the contract is based upon the general terns offered by one of the parties. This will, for instance, be the case for most consumer contracts, but is also common in business to business transactions.

A first option is to choose the courts and the laws of the country where the business offering the terms is established. This will reduce the legal unpredictability associated with doing business with several countries, and is therefore advisable in many cases.

A second option is to choose the court and laws of the country where the customer is domiciled. This will make the legal situation more uncertain for the business, since it will have to deal with several legal systems if it's potential customers are domiciled in several countries. On the other hand, it can help improve the confidence of the customer, and thereby increase the business.

A third option is to let the customer make a choice, but limit the choice to a few options that the business finds acceptable.

Tips for choice of law and jurisdiction clauses

- **Should the contract include a choice of law and a jurisdiction clause?**

It is strongly advisable to include such clauses, since it will greatly reduce the legal uncertainty associated with determining the applicable law and jurisdiction in the absence of a choice.

- **What should the choice be?**

The parties should carefully consider the possible advantages and disadvantages of the different choices available.

- **Are the parties free to choose applicable law and jurisdiction?**

Before drafting the choice of law and jurisdiction clause, the parties should make sure that there are no special provisions that limit their freedom to choose. The parties should be particularly aware of mandatory rules offering special protection to consumers.

- **Should the business be limited to certain countries?**

If there are limitations on the freedom to choose applicable law and jurisdiction, the business runs the risk of having to deal with several legal systems, and of facing court proceedings in several countries. In such case, it may be considered if the business should be limited to certain countries.

- **Alternative dispute resolution**

When considering the choice of law and jurisdiction clause, the parties should see this question in connection with the possibility of also including an ADR agreement/clause.

- **Seek professional legal advice**

It is advisable to seek professional legal advice to draft the choice of law and jurisdiction clauses. It is important to determine if the parties' freedom of choice is subject to restrictions, and to ensure that the relevant clauses are drafted clearly and unambiguously.

CHECKLIST CONTRACTUAL STEPS

This checklist deals with some suggestions as to the structure of a consumer contract concluded via an interactive website

STEPS/OVERVIEW

- E-catalogue or shop-window
- First click, drag or similar action for choosing one or more products
- Recapitulative page
- Second click for sending the binding order
- Acknowledgement of receipt from the e-supplier

The customer should be given information on the significance of each step, ie is should be clear at what point he or she has given the order. Also, the process should allow to correct any errors.

THE E-CATALOGUE

It is important that the contracting process is structured in such a way that the website is only an e-catalogue, or in legal terms, an invitation to treat and not a binding offer. This avoids the supplier being bound by a customer order having still the opportunity to check stocks or correct errors. Suppliers should be aware that advertising regulations apply to their e-catalogue and should consider that their site is accessible from all jurisdictions.

THE FIRST CLICK

The e-commerce platform should have built in at least a two click process to avoid inadvertent clicking by the customer. The non-binding nature of the first click should be clearly indicated to the customer. A presentation of a shopping cart or similar device would illustrate this.

THE RECAPITULATIVE PAGE

The recapitulative page should contain a summary of the products including a description of the products (rather than just a code number) and including weight, colour and other characteristics. This description is necessary to exclude any errors. Therefore a button (or a similar device) should allow the cancellation of the total purchase or of one or more products. Furthermore, an opportunity to correct the quantity of products or of their characteristics should be given.

THE SECOND CLICK

It should be made clear to the customer that this is the sending of the order- the use of a button described order, buy or purchase may serve this purpose.

THE ACKNOWLEDGEMENT OF RECEIPT

By law the supplier is obliged to send to the customer an acknowledgement of the receipt of the order. This has to be done without undue delay. It could be worded something like "we confirm that we have received your order".

INFORMATION TO BE PROVIDED

Prior information-information to be given at the outset
The following information must be given before the contract is concluded:

- the supplier's name (and in the case of advance payment also his address), Article 4 (1) (a),
- the main characteristics of the goods or services, i.e. essentially a description of the goods or services, Article 4 (1) (b),
- the price including all taxes (VAT) and all delivery costs, Article 4 (1) (c) and (d),
- the arrangements for payment, delivery or performance of services, Article 4 (1) (e),
- the existence of a right of withdrawal, unless the sale is exempted from that right, Article 4 (1) (f),
- if the consumer is to use a premium rate telephone number the cost of the call must be specified, Article 4 (1) (g)
- how long the offer or the price remains valid, Article 4 (1) (h)
- where there is a continuous supply (e.g. mobile phone, cable/satellite TV, gas or electricity) or where there is a recurring supply (e.g. a monthly book or CD club) the minimum duration of the contract, Article 4 (1) (i).

Information which must be confirmed
With the exception of the last three items (premium rate, duration of the offer and minimum duration of ongoing contract), the information must be confirmed in writing or in another durable medium unless it has been given in writing or another durable medium from the outset. Thus, the information items in Article 4 (1) (a)-(f) must be confirmed in writing or another durable medium. In addition, the following information must be included in this confirmation:

- the details about when and how the consumer can exercise the right to cancel
- a geographical address to which the consumer can address any complaints
- if the supplier provides any after-sales services or guarantees, the details of such services and guarantees
- if the contract is for a service with no specific end date or for a period longer than a year (e.g. mobile phone, satellite/cable TV, gas or electricity), the supplier must provide details on how to cancel the contract.

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 4

Consumer Protection Issues for ISPs

CHAPTER 4

4. Consumer Protection Issues for ISPs

4.1 Objectives

The relevant texts adopted at the European level, or at a draft stage, concerning the protection of consumers on the Internet are the following:

- The ***Distance Contracts Directive***[8], one of the major texts providing protection to consumers when they conclude a contract at a distance, including on the Internet. Although this text is not especially aimed at electronic contracting, it brings important provisions ensuring, among others, that reliable information is provided to the consumer, both before and after the conclusion of the contract, a right of withdrawal allows the consumer to renounce to the contract without penalty and without giving any reason, and that the performance of the contract takes place within a reasonable period. This Directive will be complemented by a draft Directive on distance financial services, the Proposal for this has been adopted on 14 October 1998[9];
- The ***Recommendation on Electronic Payment Instruments***[10] that provides interesting provisions regarding the liability of the parties, i.e. the holder and the issuer of a payment instrument;
- The ***Council Resolution*** on the *Information Society Aspects Concerning Consumers*[11]: that acknowledges the impact of the new technologies on the daily lives of the citizens and the potential advantages consumers can get from the new Information and Communication Technologies, and that stresses the necessary provision of an *equivalent protection* regarding the new technologies;
- The ***Directive on certain legal aspects of information society, notably of electronic commerce, in the internal market***[12] of 8 June 2000, where consumer protection is dealt with: the directive raises, among others, the issues of commercial communications distributed through the network, general information to be provided, electronic contracts, placing of an order, and applicable law. This text is a step towards a specific protection of consumers on the Internet;

---

8 Directive EC/97/7 of the European Parliament and the Council on the protection of consumers in respect of distance contracts, 20 May 1997, *OJEC* L 144 of 4 June 1997. For further developments on the Directive, see SALAÜN A. *Electronic Commerce and Consumer Protection*, at http://www.droit.fundp.ac.be/textes/consumer.pdf

9 Proposal for a Directive concerning the distance marketing of consumer financial services COM (1998) 468 final, http://europa.eu.int/comm/dg15/en/index.htm

10 Recommendation of the European commission concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, 30 July 1997, 97/489/EC.

11 Resolution of 19 January 1999 (1999/C 23/01) *OJCE C* of 28.01.1999 p.23.

12 Directive 2000/21/EC of the European Parliament and the Council of 8 June 2000, *OJEC*, 17.7.2000, L 178/1.

- The ***OECD draft recommendations*** of the Council concerning guidelines for consumer protection in the context of electronic commerce of September 1999[13]: those recommendations stand apart by promoting initiatives from the private sector: the necessary tools for ensuring confidence in the digital marketplace should be developed by businesses, along side any legislative action;
- The ***Directive concerning misleading advertising*** so as to include comparative advertising[14];
- The ***Directive on the sale of goods and associated guarantees***[15];
- The Directive on ***unfair contract terms*** in consumer contracts[16].

4.2 Core Principles

4.2.1 What is a Consumer?

According to the European Directives, a consumer is understood as ”any natural person who is acting for purposes which are outside his trade, business or profession”.

4.2.2 What is a Distance Contract?

The Directive concerning the protection of consumers in respect of distance contracts defines the distance contract as ”any contract concerning goods or services concluded between a supplier and a consumer under an organised distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded”.

4.2.3 Transparency

The obligation of transparency in the context of electronic commerce with providers and consumers is of crucial importance. The international character of the network, the electronic character of the means of communication used, the rapidity for concluding a contract, all imply a totally different way of buying goods and services at a distance. As a response to this situation, a fundamental principle of transparency in both pre-contractual and contractual relationships should apply. Transparency should challenge these particular characteristics of electronic commerce and give an answer to a concrete need of information.
Therefore, the principle of transparency should apply to the business, namely the professional himself and his activity; to the goods and services proposed by the provider; to the conclusion of the contract and to the performance of the contract. All these principles are taken over in the distance contracts and the e-commerce directives.

---

13 Document DSTI/CP(98)4/REV6, at the occasion of Paris conference, 9-10 September 1999, available on the OCDE Website: http://www.oecd.org

14 Directive 97/55/EC of European Parliament and the Council of 6 October 1997 amending Directive 84/450/EC, *OJEC L* 290 of 23.10.1997.

15 Directive 1999/44/EC of 25 May 1999

16 Directive 93/13/EC of 5 April 1993, *OJEC L* 95 of 21 April 1993.

4.2.4 Fair Business Practices

In the same spirit, the particularities of electronic commerce call for a strengthening of fair business and commercial practices. Besides transparency as to the practices of the providers, it is important that the business practices, as they are described in national or European legislation, are strictly and fairly complied with.
Two particular fields are concerned by these fair practices in the frame of contracts with consumers: commercial communications and distance contracts.

4.2.5 Trust and Confidence

Both the transparency principle and the fair business practice principle follow the same objective: to provide consumers with a context of trust and confidence where they feel confident to buy goods and services. Such a context can be developed, on the one hand, by fulfilling the obligations of transparency and fair business practices as described above, but, on the other hand, further commitments can be made by providers like adhering to codes of conduct or site labelling initiatives, or providing an on-line dispute resolution mechanism.

4.3 Recommendations

4.3.1 In the Field of Transparency

The notion of transparency implies that the information is provided in a clear and comprehensible manner: the technique should not be used to hide any information. The e-commerce directive imposes businesses to make information easily, directly and permanently available on their websites.

4.3.1.1 Transparency as to the Business

This information should be available on the website as soon as the consumer enters the site, irrespective of a purchase.

In particular, the provider should make available on his website the following information:
- his name and geographical address of establishment,
- his address, as well as an e-mail address where the consumer can easily reach him,
- if applicable, the trade register where he is entered and his registration number,
- if applicable, the activities subjected to an authorisation scheme,
- if the profession is regulated, the order, title and applicable rules,
- if applicable, his VAT number,
- the prices of the information society services.

This information is aimed at bringing trust and confidence in the consumer's mind as to the identity of the provider and his professional activity.
The e-commerce directive encourages that the information on codes of conducts the provider subscribes to is given, as well as the mean to access such codes.
Moreover, one can add to these compulsory information the following information:

- a link to the *Certification Authority's* website where the provider holds a certificate,
- a link to the *data protection authority* where the provider is registered,
- a link to the *labelling authority* where the provider is registered.

4.3.1.2 Transparency as to the Proposed Goods and Services

Content of the Information

Warnings:

1) this information should be available on the site as soon as the consumer enters the site, irrespective of a purchase;

2) this information should be accessible at any step of the transaction (e.g. through an icon or a link), allowing the consumer to access at any step of the visit.

According to the directive on distance contracts, the information on the goods or services proposed should at least contain:

- the main characteristics of the goods or services,
- the price of the goods or services including all taxes,
- delivery costs, where appropriate,
- the arrangements for payment, delivery or performance,
- the existence of a right of withdrawal,
- the cost of using the means of distance communication, where it is calculated other than the basic rate,
- the period for which the offer or the price remains valid,
- where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

Additional Information

Where the good or service ordered by the consumer is 'immediately consumed' - in other words when it is directly downloaded on his computer- it is recommended to provide *additional information* to the consumer, when the technology permit this. Such information should enable the consumer e.g. to check the compatibility with his own software, in order to avoid technical incompatibilities.

Sample

Where the technology permits, a *sample* of the product should be sent to the consumer. The sending of an indicative piece of the product brings the advantage of placing potential purchasers in a context of confidence since they are able to receive, free of charge, a sample of the digitised good they might be reluctant to buy without this prior check. After receipt, the recipient should feel confident in ordering the product if it is in accordance with the characteristics described in the offer and technically compatible with his own system.

4.3.1.3 Transparency as to the Conclusion of the Contract

Before the Contract is Concluded: Access to the Contractual Terms and Conditions

The contractual terms and conditions should be made easily accessible to the consumer: they should be brought to the consumer's attention in order to ensure that the consumer can access them.
The access to the contractual terms and conditions can be made in various ways, notably:

- a first system is the "*reference statement without hyperlink*": in that case, the provider makes a reference to the contractual terms and conditions and invites the consumer to ask copy of these terms and conditions by mail or by e-mail. This reference should appear at the bottom of the order form in bold character with a winking sign;
- a second system is a "*reference system with hyperlink*": it permits the consumer to click on the hyperlink and to have an automatic access to the web page containing the contractual terms and conditions;
- a third system is a "*dialogue box*": it automatically invites the consumer to go through the terms and conditions before the order and the conclusion of the contract.

This last system is obviously the most satisfactory one, since it ensures that the consumer has previously accessed the contractual terms and conditions before submitting the offer. Furthermore, this system complies with some national legislation that make compulsory the access by the consumer to the contractual terms and conditions before the contract is concluded.
The E-commerce Directive provides that the contractual terms be provided to the consumer in a way that enable them to save or print the terms.

Before the Contract is Concluded: Steps to Conclude the Contract

The provider should inform the consumer on the manner the contract is to be concluded, notably the different steps to follow to conclude the contract, and on the means to correct handling errors. The E-commerce Directive obliges the provider to acknowledge receipt of the order of the consumer.
Furthermore, a *summing up* of the transaction should systematically be proposed to the consumer before he engages himself in the contract. This final summing up should allow a visualisation of all the characteristics of the contract. It should obviously enable the consumer to bring rectification to the content of the contract. This enables the consumer to correct any input errors of necessary.

Once the Contract is Concluded: Confirmation of Information

The provider should provide the consumer with a confirmation of the information. This confirmation should be sent in a separate *e-mail*, with a prior check that the consumer owns a personal e-mail address, if not - for example if the consumer is connected via a public place e.g. a *cybercafé* - the provider should find another means agreed with the consumer, to enable him to receive the confirmation. Confirmation can also be made on a web page, but the problem is that it is up to the consumer to make this document durable (by saving or printing the information), although the obligation to make the confirmation durable lies on the provider.

The confirmation must contain:

- the conditions and procedures for exercising the right of withdrawal,
- the geographical address of the place of business of the supplier to which the consumer may address any complaints,
- information on after-sales services and guarantees which exist,
- the conditions for cancelling the contract, where the contract is of unspecified duration or a duration exceeding one year.

Once the Contract is Concluded: Recording of the Transaction

In order to guarantee a means to prove the transaction and its content, a recording of the transaction should be provided to the consumer. It could be sent to the consumer through a similar medium than the one used for the confirmation of information (to guarantee the validity and integrity of the recording, electronic signatures could be used).

4.3.1.4 Transparency as to the Performance of the Contract

Payment

Information should be provided on the payment system used by the provider: the level of security of the payment system proposed should be briefly described. Information should also focus on the related fees, charges or handling costs incurred by the use of a particular means of payment.

Performance of the Contract

The provider should duly inform the consumer on the way and the period of performance of the contract.

4.3.2 In the Field of Fair Business Practices

Providers engaged in electronic commerce should pay due attention to the interests of consumers and act in accordance with fair business and marketing practices. They should not use unfair contract terms in their contracts with consumers.

4.3.2.1 Commercial Communications

Identification

Both the *commercial nature* of the communication and the *person* for which the communication is made should be clearly identified. In the case of commercial communications through e-mails, the commercial nature should be identified as soon as the message is received by the consumer, which allows the consumer to use filter services.

Right of Objection

The provider should comply with the lists and registers where consumers show their objection to receive commercial communications through e-mails (*opt-out* principle).[17]

4.3.2.2 Distance Contracts

Right of Withdrawal

The provider should offer the consumer a right to withdraw from the contract, free of charge and without giving any reason. The only costs that can be borne by the consumer are the direct return costs of the good. Contracts falling into the exception to the right of withdrawal should comply with the exceptions set forth in either the national legislation or the European one.

The period for which the right of withdrawal is valid should rely on the relevant national legislation, and should not be less than 7 working days.

Reimbursement

Where the consumer uses his right to withdraw from the contract, and where he has already paid the amount of the contract (totally or partially), the provider should reimburse him the sums he has paid in a short delay.

Performance of the Contract

The provider should perform the contract within a maximum of 30 days, except if otherwise agreed by the parties.

[17] The Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector contains provisions that unsolicited communications may only be sent where the user has previously consented.

4.3.3 Increasing the Consumer's Trust

The provider has the possibility to commit himself in initiatives aimed at providing trust and confidence in electronic commerce.

4.3.3.1 Codes of conduct

Adhering to a code of conduct adopted by a professional organisation or a public authority shows the commitment of the provider to go forward with legislation and to commit himself in complying with additional rules, specifically devoted to a sector of activity.

4.3.3.2 Site Labelling

Site labelling - understood as the combination of technology and audit procedures with the aim of answering consumers' expectations with regard to electronic commerce - can complement the legislative action protecting consumers though a specific answer to on-line consumer issues. It can participate in the development of a context of confidence, provided some conditions are complied with, notably:

- that suitable information is available on the site regarding the label and its meaning,
- that the labelling authority fulfil the criteria of independence and expertise,
- that effective and relevant criteria are defined as the basis of the labelling initiative,
- that effective and regular controls are operated on the compliance with the criteria defined.

4.3.3.3 ADR

As a supplement to the labelling initiative, a further step in the protection of consumers can be reached by offering an on-line alternative dispute resolution mechanism (ADR). This can either be linked to a labelling initiative (as a sanction in case of non-compliance with the criteria), or can exist beside site labelling. In both cases, it is aimed at providing consumers with a quick, affordable solution, tailor-made to the network, to solve disputes arising on the network with the provider or any other intermediary. Here again, minimal requirements should be complied with in order to participate in the development of a context of confidence: those requirements relate to the information that should be provided to the consumer; to the necessary explicit consent of the parties to submit their dispute to an ADR; to the neutrality of the third party asked to solve the dispute and to the compliance with legal requirements concerning consumer protection.

TIP- Link to Trustmark providers

http://www.budget-net.com/bnet/webtradersite/code_uk.html
www.dedigitaleconsument.nl
http://www.which.net/webtrader/
www.truste.org
http://www.cpawebtrust.org/
http://www.trustuk.org.uk/
http://www.dma.org.uk/thedma/cgi-bin/incorporate.pl?fname=../documents/standards.txt&doctype=stand
http://www.trustedshops.com/en/shops/obligations_en.html
http://www.aece.org/corporativo/sello.htm

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 5

Payment Methods- Legal Issues

2 CHAPTER 5

5. Payment Methods- Legal Issues

5.1 Fraudulent Payments

5.1.1 Who accepts the loss where a fraudulent payment is made?

- Carefully check the terms and conditions of the payment contract with the issuer, whether it is a credit card company or an electronic money institution, to determine whether the service provider will be obliged to refund the value of a transaction to the issuer should a payment be fraudulently made.
- Often in credit card contracts between the issuer and the service provider the issuer will provide that where there is a 'cardholder not present' (remote) transaction then the service provider will have to accept the risk. As a result the retailer may not receive the full value of the transaction if a payment is disputed and the credit card issuer refunds the disputed amount to the customer.

5.1.2 What can you do if the risk is placed with the service provider?

- In most of the Member States contracts between businesses are not subject to any restrictions so it is up to the service provider and the payment issuer to negotiate the terms and the allocation of risk for lost or fraudulent payment messages between the parties.
- However, in the UK the Unfair Contract Terms Act 1977 restricts the use of exclusion clauses in standard term contracts where they are not considered reasonable. For example an issuer attempting to exclude itself from liability for negligence (such as not cancelling a credit card on notification of its loss) or breach of contract would likely be considered to be an exclusion clause.

5.2 Data Use and Security

5.2.1 Are there restrictions on the service provider's use of payment information?

- Payment data such as the credit card name, number and address is personal data. Service providers collecting and processing personal customer data will be subject to the data protection principles laid down in the Data Protection Directive.
- Service providers must ensure that they do not use the payment data collected for purposes other than those which have been registered with the Data Protection Commissioner. For example the information cannot be used for marketing purposes without consent from the data subject.

5.2.2 What security measures should be taken to protect payment data?

- Service providers who set up a database of customer payment information (credit card details) in order to speed-up future purchases should take care to ensure the security of the database.
- Make sure that 'appropriate technical measures' are used to prevent unauthorised or unlawful processing of personal data or accidental loss, destruction or damage of the data. This means that encryption and security measures such as SSL should be used when transferring data between parties and that access to the contents of the database should be strictly controlled.
- Careful monitoring of the system will also ensure that adequate security is maintained and technical measures are updated as and when necessary.

5.3 Electronic Money Issuer

5.3.1 How is the issuance of electronic money regulated?

On implementation of the EU Electronic Money Directives which is due by the end of April 2002 any institution issuing electronic money will have to comply with the provisions of the directives. These include the following:

1. Authorisation and verification of activities by a competent authority (generally the central bank, in the UK the Financial Services Authority)
2. An initial capital requirement of 1 million euros and on-going funds requirement of at least 2% of outstanding liabilities;
3. Restrictions on investments - only very low risk investments.

5.3.2 What steps must be taken to identify customers?

- To comply with the Money Laundering Directive issuers must adequately identify customers opening electronic money accounts online.
- They must also follow certain procedures such as record keeping, identifying clients and reporting any suspicious activities.

5.3.3 Are there restrictions on the use of customer details?

- When collecting and using personal customer data the issuer must comply with the Data Protection Directive.
- The issuer must register the purposes for which the data has been collected with the national data commissioner.
- Any processing of the data which includes obtaining, recording, holding consulting, disclosing or erasing of the data must be carried out in accordance with the data protection principles.
- Issuers must carefully consider the purposes for which the data is collected. This data cannot be used for purposes other than those for which the issuer has registered. The data subject must be aware of the purposes and data must not be processed unless:

1. The data subject has consented.
2. It is necessary for the performance of contract.
3. It is necessary to comply with legal obligations, public sector purposes or the legitimate interests of the data controller unless this would prejudice the rights of the data subject.

- Potential problem areas for issuers are the use of data for other purposes such as marketing, the transfer of data to countries outside the EEA and securely holding and transferring the data.

- In many cases the issuer can ask the user to consent to the use of information for marketing purposes but the issuer should be aware that the consent must be 'freely given', 'specific and informed'. The data subject must therefore be provided with a clear explanation of the purposes for which the data will be used, which may include the form of marketing intended and he or she must have actively consented. 'Opt-out' boxes will not generally be sufficient.

5.3.4 Are there restrictions on the terms which can be incorporated in the contract with the consumer?

- There are various consumer protection regulations which have been developed to protect the consumer from being bound by unfair terms which are clearly to his or her detriment.
- As regards electronic payments, in addition to the general consumer protection rules there are also some specific rules which relate particularly to the terms and conditions of contracts relating to payment instruments and electronic money.
- Issuers should be aware that the rules currently vary in the different Member States.
- To ensure that the service provider's law will apply in the event of dispute a choice of law clause should be inserted (assuming the service provider does not choose to elect another country's law). Likewise a choice of jurisdiction clause should be incorporated to ensure that any dispute will be heard in the courts of the country of the service provider. (Note that consumer protection provisions will mean that in certain cases these may not be effective.)
- Issuer should take into account the following regulations and check that there are no relevant national regulations or codes.

5.3.5 The EU Directive on Unfair Terms in Consumer Contracts

- The EU Directive on Unfair Terms in Consumer Contracts prevents an issuer from binding the consumer to terms which are unfair. The Directive provides that 'a contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'.
- The inclusion of a term by an issuer which places all of the liability on the consumer for any unauthorised transactions is likely to be considered unfair and would therefore be invalid.

5.3.6 Distance Selling Directive

- The Directive provides that if there has been fraudulent use of a payment card in a distance sale then the amount must be reimbursed to the customer.

5.3.7 The Payment's Recommendation 1997

- As it stands the Payments Recommendation is not binding but many of the provisions have been implemented in the various Member States to some degree. Furthermore the provisions of the Recommendation may in the future form the basis of directive and therefore become binding.

- An issuer should in particular consider the following provisions:

1) The holder (the consumer) is not liable if a payment instrument is used without physical presentation or electronic identification (of the instrument itself).

2) The burden of proof to show that a transaction has not been affected by technological errors should be on the issuer.

3) The issuer is liable for unauthorised or defectively executed transactions.

4) The issuer must provide information in the official language of the Member State in which it is

5.3.8 Proposed Distance Marketing of Financial Services Directive

- Prior to conclusion of the contract, the consumer should be informed of the following:

a) the identity and address of the service provider;
b) cost of the services including tax;
c) a description of the services;
d) arrangements for payment, delivery or performance;
e) information on cancelling the contract;
f) the terms and conditions of the contract in writing or in a 'durable medium';
g) information on the right of withdrawal from the contract.

- No unsolicited distance supplies of financial services should be made.

5.3.9 Relevant National Provisions - UK

- In the UK there are some restrictions on the terms to which the stronger party can bind a weaker party. This applies only to exclusion clauses where The Unfair Contract Terms Act 1977 places restrictions on the use of exclusion clauses in standard term contracts where these are not considered to be reasonable. Reasonableness is determined taking into account all of the relevant circumstances including:

a) the resources which an issuer could expect to be available to him or her for the purpose of meeting the liability should it arise;

b) how far it is open to the issuer to cover any losses by insurance.

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 6

Principles of Taxation in E-commerce

CHAPTER 6

6. Principles of Taxation in E-commerce

6.1 Direct Taxation

6.1.1 Allocation of Income / Tax liability

Taxpayers are generally taxed on their world-wide income in the state where they live. Most states also tax income earned within their territory by foreign taxpayers. These two ways of taxing income are, in an international context, referred to as 'residence-based' taxation and 'source-based' taxation. If income is taxable in two states having concluded a double taxation treaty, the treaty provisions assign the right to taxation to one of the signatory parties: either to the state of residence or to the source state. For taxpayers taxation in the source country means compliance with a foreign tax regime and application of the tax bases and rates of the source state. The effects of the latter point depend on whether the source state provides for a higher or a lower tax level than the state of residence.

Generally speaking, the state of residence has the right of taxation. There are two exceptions of specific importance in the field of electronic commerce: business profits derived from the activity of a permanent establishment and withholding taxation of royalty payments.

6.1.2 Permanent Establishment

Business profits are taxable in the source state when they are attributed to a permanent establishment there. The principle of permanent establishment was developed in a physical world and thus is difficult to apply to electronic commerce activities.

A website does not involve any tangible property and therefore cannot itself constitute a permanent establishment. It leaves only the server as a possible nexus to the source country.

It is not relevant whether the equipment is or is not operated and maintained by personnel in the source country.To constitute a permanent establishment the server must

- be owned or rented by the content provider,
- be located at a certain place for a sufficient period of time, and
- include activities that form in themselves an essential and significant part of the commercial activity of an enterprise as a whole, i.e. at least accept orders but more likely also deliver goods or services electronically.

A server or other equipment operated by an Internet service provider (ISP), providing only or *inter alia* access to the Internet, will in most cases be regarded as permanent establishment.
It could be possible that an ISP constitutes a permanent establishment of the enterprise that caries on electronic commerce through websites operated through the servers owned and operated by these ISP's. Therefore the ISP must constitute an agent for the enterprise.

6.1.3 Withholding Taxation of Royalty Payments

Art 12 para 2 Model convention defines royalty as : " payment of any kind received as a consideration for use of, or the right to use any copyright of literary, artistic, or scientific work including films [...]".

Generally, the state of the beneficial owner's residence is entitled to the exclusive taxation of royalty income. However, several EU and non-EU countries have reserved the right to tax royalties at source in some way. The transfer of the full ownership of the rights in the copyright do not represent a royalty. Payments made for the acquisition of less than the full rights in the copyright will represent a royalty where the consideration is for licenses to reproduce and distribute to the public software incorporating the copyright programme, or to modify and publicly display the programme, and similar arrangements.

Reproducing rights which do no more than enable the effective operation of the programme by the user, for instance copying onto the hard drive or the random access memory or making an archival copy, shall be dealt with as commercial income and thus be taxed in the state of residence. Even payments for 'site licenses', 'enterprise licenses' or 'network licenses' which

are necessary to operate the programme within a business or network will generally not be regarded royalties.

6.1.4 Arm's Length Principle / associated companies

This standard assumes that the allocation of profits between affiliates equals the profit allocation between third parties for the same or similar supplies under the same or similar conditions. The starting point for any transfer pricing analysis seeks to identify the different contributions to a transaction made by the affiliates of a global trading business and to reward them using the comparable uncontrolled price method, the cost plus method and the resale price method which are referred to as the 'traditional methods'.

Basically, this standard applies to transactions between associated companies. Nonetheless, it serves also in apportioning income between a permanent establishment and the head office or other permanent establishments. For SMEs carrying out electronic commerce that means that they have to determine and to document appropriate transfer prices using the traditional methods when e.g. licensing the right to distribute software to an Internet marketing subsidiary set up abroad.

6.2 Practical reference

6.2.1 Tax Treatment of Website Cost

Please note that the national auditing standards are virtually not harmonised. Moreover, in several countries International Accounting Standards may be applied or even U.S. General Accepted Accounting Principles. Furthermore, national tax laws may provide for specific rules regarding auditing for tax purposes.

1. The standard website regarding digital marketing should be considered one asset. Additional data such as intangible products intended to be sold via the Internet, specific short term information, e.g. special offers, events, career opportunities will normally be regarded as separate assets or rather as expenses which are immediately deductible.

2. The basic website or other assets with an ordinary useful life of more than one year, e.g. the electronic catalogue 1999/2000, are considered intangible assets.
3. In some countries intangible assets which have been created within the enterprise may not appear in the balance sheet. Thus, if this is the case or a web designer created the asset in the framework of a temporary service contract the cost will be deductible in the year in which they occurred.
4. If, however, the website or another asset is created by a web designer who acts under an agreement to bring about a specific result the asset will appear in the balance sheet. Its value equals the acquisition cost.
5. The value of an asset which must be activated can be deducted in the way of depreciation over the asset's ordinary useful life. The ordinary useful life of a website or related assets must be determined on a case by case basis. Conservative approaches tend to assume a period of three years where websites are regarded.
6. Even more important is the tax treatment of maintenance cost. This cost can usually be deducted in the year of occurrence unless the basic structure of a website is redesigned or a new separate asset is created. The possibility of immediate deduction exists regardless of whether the maintenance is carried out by the enterprise's own staff or an independent contractor.

6.2.2 Separate Entity for Internet Distribution

In case of established enterprises economic reasons might exist to set up a separate entity for the distribution of products via the Internet (generally referred to as outsourcing). Such a subsidiary can be located in the same jurisdiction as the parent company or abroad.

1. Setting up a separate entity one has to take into account that corporate restructuring operations under most tax systems give rise to taxable gains at the shareholder or company level. The more valuable the transferred assets are the higher are the potential taxable gains. This means that setting up the separate entity as a start up company for Internet distribution bears less risk than outsourcing an existing division for Internet distribution. However, there is a certain additional risk that even the fact that the parent company gives up the chance to make profit by distribution via the Internet might result in a taxable gain.

2. Most national laws exempt gains from specific forms of restructuring operations from taxation, even if companies from two or more Member States are involved. One of these cases is the transfer of assets of a branch of its activities in exchange for shares of the acquiring company. It is, however, quite doubtful that a division for Internet distribution constitutes such an independent business within the enterprise.
3. If a separate entity is founded in a non Member State the transfer of assets gives rise to taxable case regardless of whether a specific form of reorganisation is met.
4. Establishing an entity in a low tax jurisdiction can be used to reduce the overall tax burden. Establishing an entity for tax reasons one should have a close look at the income tax and, far more important, the indirect tax rates.
5. If the low tax jurisdiction is a non-treaty country the state in which the products are consumed will apply its unilateral provisions regarding taxation of non-residents. It is thus possible that according to national tax law the sale of products might trigger taxable income in that country. It is even possible that the state of residence of the parent company taxes profits generated by the subsidiary, as France does under certain circumstances.
6. Moreover, appropriate transfer pricing might, also when a treaty exists, lead to the result that only little income is derived from the distribution company. In any case the profits distributed to the parent company will be subject to tax in the state of residence of the parent company. One should therefore compare the tax sparing effects with the cost of compliance with a foreign tax system.
7. In any transaction between affiliates it is crucial to maintain proper documentation of the transfer pricing decisions. One has to bear in mind that two different jurisdictions will claim the right to tax the profit from the transaction they consider appropriate. Appropriate documentation is the main shelter against double taxation arising from such transactions.
8. It will be necessary to license the right to distribute intangibles to the separate entity. It should be taken into account that such licensing might trigger withholding taxation of royalties paid as a remuneration. In particular Portugal, Spain, Austria, Greece, Italy and the U.K. apply withholding taxes even in cases where the licensor is resident of a treaty country, e.g. another Member State.

6.2.3 Deployment of Equipment Abroad

The issues arising from the deployment of equipment abroad are to some extent comparable to the issues mentioned above. The reasons for setting up a server in another country might either be general aspects, such as accessibility, or tax planning opportunities. As most states tax their residents' world-wide income the latter argument only applies when the equipment serves as a shelter against taxation in the state of residence, i.e. can be regarded as a permanent establishment in another treaty country.

1. Taking into account the cost of compliance with a foreign tax system, such as consultancy fees, it is for small businesses generally advisable to disregard tax planning reasons for setting up a permanent establishment abroad.
2. That does not hinder the deployment of a server abroad as other ways exist to prevent from constituting a permanent establishment. The most effective one is simply to conclude a service agreement with a domestic ISP rather than setting up and maintaining an own or rented server. Such a service agreement might consist of storage of data, ensuring 24-hour access to the Internet, no physical access for the content provider, maintenance of the equipment by the ISP, who also should have the right to reallocate the data on his storage devices without restriction.
3. The deployment of a server in another Member State will most likely not give rise to a fixed establishment for VAT reasons, as the generally the place where the supplier or the customer, respectively, has established his business prevails. Where the supplier has concluded a service contract with the ISP, as described above, no fixed establishment will be considered to exist.

6.3 Indirect Taxation

6.3.1 VAT: The Destination System

As a consumption tax VAT is generally levied in the state of consumption (with regard to the supply of goods often referred to as the state of destination). This system, however, is not consistently applied. Cross-border supplies of goods and services to taxable persons are usually taxed in the state of destination whereas supplies to private customers are mainly

subject to tax in the country of origin. This basic distinction currently also applies to electronic commerce transactions. There is, however, international agreement to aim at taxing the supply of services in the field of electronic commerce in the country of consumption.

6.3.2 Practical reference

Physical Delivery of Goods

Up to now the website is in most cases used to advertise products and to conclude contracts, while the delivery is carried out by physical means. Moreover, in particular in case of digital products which can be delivered either via the Internet or in physical form on a data carrier the latter provides for a business alternative which might under certain circumstances be favourable for tax reasons.

1. Standard software on a data carrier is considered a good for VAT purposes. Customised software, however, is not.
2. The supply of goods to taxable persons in another Member State is zero-rated in the state of origin and taxable as an intra-community acquisition in the State of destination, if the supplier and the consumer have an value added tax identification number. As the recipient is liable for the payment of tax the supplier must not fulfil any tax duties in the country of destination. He must, however, submit a quarterly recapitulative statement of the acquirers in the country where he has established his business.
3. If the purchaser is a non-taxable individual the supply is subject to tax in the Member State, where the despatch or transport begins, unless the taxable amount of supplies to the same Member States exceeds 125.000 Euro in one calendar year. In cases where the threshold is exceeded the place of supply is deemed to be in the Member State where the despatch or transport ends. The supplier becomes liable to register for VAT in the Member States, where the distance-selling threshold is exceeded which may include the appointment of a VAT representative according to national law.
4. Supplies from non-EU countries are subject to taxation at importation. Small packages relief applies to supplies worth less than 50 Euro such as books, videos, music CDs and standard software on data carriers. Moreover, determining the taxable amount of standard software only the cost or value of the carrier medium itself may be taken into account.

This significant difference in tax treatment should be considered. To provide for both ways of delivery according to the location of the customer might provide for a competitive advantage. When setting up a separate entity for the physical delivery of goods in a non-EU country the disadvantages mentioned above in point 2 should be considered carefully.

Provision of Services Including Download of Virtual Products

1. Most electronic commerce transactions will constitute a supply of intangible services.
2. Such intangible services are supplied at the customer's place, if performed to taxable persons established in another Member State. In such cases the reverse charge mechanism applies which means that the taxable person receiving the service becomes liable for the VAT due. In some countries, such services on which tax is payable by the customer do not trigger the duty to register, e.g. in Belgium, Germany, France and Finland.
3. In other cases, e.g. the supply to non-taxable persons, the place of supply is therefore the place where the supplier has established his business. For businesses focusing on supplies to private consumers it will be advisable to set up their business or a separate entity abroad only in case of significant differences in the VAT rate and when the costs of compliance and maintenance are considerably low, considering possible drawbacks mentioned in point 2.
4. Downloading single copies of standard software or other virtual goods, such as music, literature, video and images, via a network does not give rise to the application of the reduced rate for the transfer of copyrights.
5. Certain services, such as website design and website hosting are generally taxed at the place where the supplier has established his business. Taxable persons providing these services are required to charge VAT at the rate in their Member State not only to private customers within and outside the EU, but also to taxable persons in another Member State and non-EU countries. These have to claim this tax back in the Member State of the supplier. That puts the EU-based suppliers in a substantial competitive disadvantage. However, even in such a case, a decision to establish a business outside the EU or to outsource the relevant business fields should be considered carefully, taking into account the drawbacks mentioned in point 2 and the fact that the Commission is aware of the situation and is taking steps to remove the competitive disadvantage.

6.3.3 VAT Credit Invoice System: Invoicing

The taxable person using supplies received for the purpose of his taxable transactions is entitled to deduct the VAT due from the tax he is liable to pay which results in tax liability only for the tax due on the value added by his participation in the transaction.
Every taxable person is required to issue an invoice, or other document serving as invoice, in respect of: goods and services which he has supplied or rendered to another taxable person or to a non-taxable legal person, supplies of goods under the distance sales rules and exempt intra-community supplies.
Art. 22 para. 3 lit. b) Sixth Directive requires that the invoice shall clearly state the price exclusive of tax and the relevant tax at each rate as well as any exemptions.

6.3.4 Practical reference / Issuance of Invoices

1. Even under the reverse charge mechanism the taxable supplier is required to issue an invoice. He may, however, not indicate the tax due on the supply.
2. Where the reverse charge system is not applicable to supplies to taxable persons the supplier has to consider the national invoicing requirements in order to enable the taxable customer to deduct the tax.

In several states paperless invoicing is allowed by law or regulation. The requirements, however, differ widely. Invoices transferred using EDI are currently in several Member States considered as invoices for VAT purposes allowing the recipient to deduct the tax indicated. However, it is doubtful, whether EDI or EDI derivatives such as 'Web EDI' or 'Lite EDI' will be accepted under a future common framework for electronic invoicing. For instance, in the German proposed law only the usage of digital signatures is foreseen. In a future common system the usage of advanced electronic signatures is likely to be required to ensure that the content of the message remained unchanged and to identify the issuer.

TIP: Links to taxation authorities and other sources of information

1. **UK**

http://www.inlandrevenue.gov.uk/

http://www.hmce.gov.uk/

2. **Germany**

http://www.finanzamt.de/

3. **Italy**

http://www.scaonline.it/html/primer_uk.html

4. **Spain**

http://www.aeat.es/

5. **Belgium**

http://www.minfin.fgov.be/index.html

http://fiscus.fgov.be/interfdafr/organogram/a.htm

6. **France**

http://www.finances.gouv.fr/DGI/

http://www.finances.gouv.fr/DGDDI/

7. **Greece**

http://www.mof-glk.gr/

8. **Denmark**

http://www.toldskat.dk/

http://www.fm.dk/

9. **Sweden**

http://www.rsv.se/

http://www.tullverket.se/sv/start/default.asp

10. Finland

http://www.vero.fi/index.php

http://www.tulli.fi/

11. Austria

http://www.bmf.gv.at/steuern/_startframe.htm

12. Luxembourg

http://www.etat.lu/DO/

13. Netherlands

http://www.minfin.nl/

14. Ireland

http://www.revenue.ie/

15. Portugal

http://www.dgci.min-financas.pt/SiteDGCI.nsf

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 7

Data Protection Considerations for ISPs

CHAPTER 7

7. Data Protection Considerations for ISPs

7.1 Objectives

The aim of this brochure is to provide legal assistance to SMEs when setting up an Internet business within the European Union. The objective is to raise some of the issues that arise from the processing of personal data and to provide some practical recommendations for businesses when processing personal data. The recommendations are divided into recommendations aimed at service providers and recommendations aimed at telecommunications operators and Internet Access Providers. The last part deals with transborder data flows and the considerations that data exporters should have when sending personal data outside the European Union.

Consumer confidence in data processing is particularly important in the development of electronic commerce. Demand for on-line services, although growing rapidly, remains fragile and concerns about privacy and security are restraining factors for consumers who might otherwise be keen on purchasing goods in cyberspace. The following recommendations therefore aim at promoting a certain number of core principles guarantors of the consumer's trust and confidence[18].

These recommendations stem from various sources such as EU directives and Council of Europe recommendations in the field of data protection (see annex). The recommendations do not exclude the respect by the SMEs of national data protection laws that might apply[19].

[18] For the elaboration of a "Privacy Policy" it is recommended to consult the Recommendation 2/2001adopted on 17 May 2001, available at http://europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm

[19] Special attention shall be paid to art. 4 of the Directive, which regulated the applicable law: *"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;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

The following core principles and recommendations are mainly derived from:

- The OECD study on the instruments and mechanisms concerning the adaptation to global networks of the OECD guidelines on data protection (DSTI/ICCP/R&G (98) 6) submitted to the group of experts of the OECD on the 17th and 18th of May 1998.
- Recommendation N° R (99) 5 of the Committee of Ministers of the Council of Europe to Member States for the Protection of privacy on the Internet, Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways (adopted on 23rd February 1999)
- The EU directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data adopted on the 24th October 1995.
- The EU directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector adopted on the 15th December 1997.[20]
- Recommendation 3/97 on Anonymity on the Internet adopted by the article 29 Working Party of the European Commission on 3rd of December 1997.
- Recommendation 1/99 on Invisible and Automatic Processing of Personal data on the Internet Performed by Software and Hardware, adopted by the article 29 Working Party of the European Commission on 23rd of February 1999.
- Recommendation 3/99 on the preservation of traffic by Internet Service Providers for law enforcement purposes, adopted on 7th September 1999.
- Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union adopted on 17 May 2001.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself."

[20] The European Commission has launched a review on the current telecommunications framework in 1999. One of its consequences is a Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. It aims at adapting Directive 97/66/EC mainly to the Internet related questions as regards privacy matters. Hereinafter "the Proposal".

7.2 Core Principles

The development of electronic commerce activities in Europe will very much depend on the trust and confidence that consumers can place into the system. The protection of personal data must be seen as a way of ensuring confidence in the system for the users of a service. Certain core principles must be guaranteed if one wishes to respect the data protection principles present in the European Union Member states. They can be summarised as the principle of voluntary participation of the data subject, purpose specification, quality of the data and security.

7.2.1 Individual Participation

The first principle concerns the individual participation of the persons to whom the data relate (data subject). This participation includes the possibility for an individual to know precisely which data is being recorded on him and can include the possibility for the data subject to fully control the transmission of his data. Thus an individual should have the possibility to consent specifically to the use of his data which are not strictly necessary for the payment or should at least be given the possibility to oppose such a use[21].

As concerns data processed for the purpose of direct marketing, both the European directive and the Council of Europe recommendation lay down an opting out mechanism[22]. Indeed the data subject is granted with the right to object free of charge to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or to be informed before data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses[23].

21 See articles 7 and 14 of the EU directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data adopted on the 24th October 1995 (hereinafter-directive 95/46/EC).

22 The differences between an “opt-out system” and an “opt-in system” rely mainly in the way the data controller has to interpret the silence of the data subject. In the “opt-out system” the silence of the data subject means that the data controller can process his personal data. In the “opt-in system” the controller needs the specific and explicit consent of the data subject to be able to process his data.

23 See article 14.b of directive 95/46/EC or recommendation 4.2. of R (99)5

7.2.2 Purpose Specification

The second principle implies that the purpose for which the data is being processed must be determined and that the data must not be processed for purposes incompatible with those for which the data was initially collected.

This principle means that the purposes for which the data is being processed must not only be determined but must also be explicit in the eyes of the data subject[24]. This implies that the data subject be informed of the purposes for which the data is processed, but also of the persons processing the data[25]. This is not only a concern for privacy but equally a consumer protection issue: in order to make informed decisions about the purchases they may make on the Internet and the means they use in order to pay for such purchases, consumers require adequate information.

The purpose for which the data is being processed must also be legitimate[26], i.e. in the case of processing of personal data in the context of electronic commerce transactions, the data must only be processed for the purpose of carrying out the service and to enhance the quality of the service. Purposes include the processing of personal data in order to render and bill the service, and services linked to the payment such as verification activities and processing to ensure the security of the payment.

Finally, the subsequent secondary purposes for which the data are used should not be incompatible with the original purposes for which the data were collected.

7.2.3 Data Quality

According to this principle the data must not be excessive in relation to the determined purposes for which they are being processed[27]. This implies that the controller must not process any further data than that which is necessary, and that there may be no excessive data (even if this data is useful). The proportionality of the data must be assessed for each finality. Furthermore the data may not be kept for longer than necessary for the purposes for which the data was collected. The data must also be accurate, complete and kept up-to-date[28].

[24] See article 6 of directive 95/46/EC.
[25] See articles 10 and 11 of directive 95/46/EC.
[26] See article 6 and 7 of directive 95/46/EC.
[27] See article 6.1.c of directive 95/46/EC.
[28] See article 6.1.d of directive 95/46/EC.

7.2.4 Security

Both the general directive and the telecommunications directive[29] require the adoption of appropriate security measures both by the controller and by the provider of a publicly available telecommunications service[30]. These technical and organisational measures must protect the personal data against any accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular when the processing of the data involves the transmission over a network[31]. The measures must ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data[32]. This requirement is clearly in line with a more general need of being able to carry out payments in a secure environment.

It must be stressed that the international nature of the Internet increases the risks for the data subject since the data could be transferred to countries that do not provide for any type of protection of personal data.

7.3 Recommendations for Internet Service Providers

The objective here is to present clear and predictable recommendations for service providers

The term **personal data** means any data relating to an identified or identifiable person. Is qualified as "identifiable" a person who can be identified directly or indirectly in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, including his behavioural identity revealed by his use of electronic commerce (e.g. telephone numbers, e-mail addresses).

The term **user** means any person, natural or legal), or association of persons making use of electronic commerce services.

The term **service provider** means any natural or legal persons or association of persons who make available either their own or third-party services.

The **data subject's consent** shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

[29] The EU directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector adopted on the 15th December 1997.

[30] The Proposal replace "telecommunications service" by "communications services", article 4.

[31] Examples of these technical measures are: crytography, firewalls, etc

[32] Article 17 of directive 95/46/EC and article 4 of telecommunications directive 97/66/EC.

7.3.1 Opposition to Commercial Communications

1. The data subject must be given the right:
- Not to receive unsolicited commercial messages;
- To object to the processing of his/her personal data for commercial purposes.

2. In order to be able to effectively exercise this right, the data subject must be informed of his right and mechanisms must be put into place to enable him to effectively object (on request and free of charge).

The first commercial communication sent to the consumer should contain information on the possibility to refuse receiving such messages, and on the steps to take in order to do so.

7.3.2 Collection of Personal Data

Limitations on the Collection and Use of Personal Data

1. Personal data can only be collected and processed by providers if permitted by some law or if the data subject has given his consent.

Consent can be declared electronically if the provider ensures that: such a consent can only be given by a deliberate and unambiguous act by the user, the consent is recorded and text can be obtained at any time and cannot be modified without detection and that the user is identified[33].

2. The provider may not make the rendering of a service conditional upon the consent of the data subject to the effect that his data may be processed or used for other purposes.

3. Personal data must be collected by fair and lawful means. This implies a maximum of transparency in the collection of the data that should not be carried out without the knowledge of the data subject.

4. The design and selection of technical means shall be configured so as to collect and use no personal data or as little as possible.

Information to Be Given to the Data Subject at Time of Collection of Data

A certain amount of information must be given to the data subject. It is recommended that the information be provided directly on the screen before the collection of the data in order to ensure the fair processing.

[33] See Germany's Teleservices Data Protection Act, August 1st 1997, §3 (7).

Users must be informed at least of :

- the purpose of collection and use of personal data,
- the name, title, address and telephone number etc. of the manager or agent within the holding enterprise concerned with the personal data,
- the obligatory or optional nature of the information requested,
- the recipients or categories of recipients of the collected data,
- the existence of a right of access and rectification,
- the existence of a right to oppose any disclosure of the data to third parties for purposes other than the requested service.

In the case of automatic data processing, in particular in the case of the use of cookies, which enables the identification of the data subject, the data subject must be made aware of the use of these means before they are actually carried out. In this case the information could be provided using the technique of a “pop up” window.

Privacy policy including complete information on the way the data is processed and the policy of the company as concerns personal data should be directly accessible from the home page of the site and anywhere where personal data are collected.

A privacy policy can contain information such as :

- the risks that the use of electronic commerce networks can incur for the protection of privacy. The risks can concern the integrity of the data, their confidentiality, security of the network or other dangers concerning the protection of data such as the collection of personal data without the data subject’s knowledge.
- the disclosure of personal data to countries outside the European Union, when there is a risk that the data will be processed in this third country for other purposes than transit purposes.
- the level of security in all the processing stages and the technical means the user can lawfully use to reduce the risks concerning the security of the data.

The provider who adheres to a privacy statement or a sectoral code of conduct must provide a hyperlink to the text of the agreement along with reference to the web site of the organisation in charge of applying and monitoring the respect of the agreement.

7.3.3 Use of Personal Data

Limitations on the Use of Personal Data

1. The provider may only process personal data to the extent that the data is necessary for the conclusion and carrying out of the contract with the user, including the billing.
2. The use of personal data for the purposes of direct marketing by the provider himself or by another provider may only be carried out if the user has been fully informed of this use and that he has consented to such a use.
3. Personal data may only be used and stored to the extent necessary for the use and billing of the service and for consumers to be able to challenge the billing. The personal data must in any event be erased not later than 3 months from the dispatching of the invoice unless the request for payment is disputed within this period or the invoice has not been paid despite a demand for payment.

7.3.4 Disclosure of Personal Data

1. The disclosure of personal data shall, in principle, be limited within the scope of the purpose for which it was collected.
2. The disclosure of personal data within the scope of the collection purpose shall be carried out with prior consent of the individual or by giving the data subject an opportunity to refuse prior to disclosure. This shall not apply however in the cases given below:

- If the personal data is disclosed to a recipient to whom the data subject has given consent that the data will be disclosed when the data was initially collected.
- If the personal data is disclosed to a recipient with an accompanying guarantee that the personal data will be handled in an equivalent manner and for the same purpose as that of the original holder through the conclusion of a contract stipulating obligations to maintain confidentiality, prohibition against redisclosure of personal data an assignment of responsibility when accidents occur in respect to the personal data disclosed.

3. When the disclosure exceeds the scope of the purpose for which the data was initially collected, the recipient must respect the principles set out in recommendations 2 & 3 must be respected unless the data subject has been notified of the information and has given his consent to the disclosure of his data for any purpose.
4. When disclosure is envisaged to a State outside the European Union, providers should inquire about of the possibility of carrying out this transfer.

7.3.5 Obligation to Manage Personal Data

Ensuring Security in the Use of Personal Data

Reasonable security measures shall be taken through both technical and organisational means against risks such as unauthorised access to personal data or the loss, destruction, alteration or leakage of personal data. Special attention must be given to data revealing particularly sensitive information.

Obligation of Employees to Maintain the Confidentiality of Personal Data

Persons engaged in the collection, use and disclosure of personal data should perform, using sufficient care, the obligation to maintain the confidentiality of the data in accordance with the instructions given by their employer.

Measures Concerning the Entrustment of Personal Data

When entrusting personal data to an outside enterprise, this one shall be selected who can handle personal data at a sufficient level of protection, and it shall be guaranteed, through the conclusion of a contract or other legal measure, that he shall only act on instruction from the manager of the initial enterprise processing the data, that the confidentiality of personal data is maintained, that re-disclosure of personal data is not permitted and that responsibility when an accident occurs is assigned.
The document referred to above shall be stored in written or in any other equivalent form, for as long as the data is managed by the outside company.

7.3.6 Respect of Rights of the Data Subject

Right of Access and Rectification

1. The user must have access to any personal data concerning him that is being processed without excessive cost and delay. If personal data is found to be erroneous following subject access, requests for correction or deletion of the personal data shall be accepted within a reasonable period of time. In such cases the recipients of the personal data shall be notified of the correction or deletion to the extent possible.
2. The right of access must not be limited to the data that the data subject himself has provided. If personal data, for example, has been generated by the use of the service, he must also have access to such data.

Right to Opt Out

Every provider who collects personal data must give the data subject at all times the possibility to opt out of the processing operation of his/her data. The possibility must be given when appropriate for the data subject to refuse certain use of his data (such as the processing of traffic data, the establishment of user profiles).

Interactivity

A direct contact with the service provider should be made possible: the provider should offer a hyperlink to consumers to enable them to make contact with him for any request of information or complaint.

7.4 Transfer of personal data outside the EU

Whilst inside the EU the level of protection given to personal data is harmonised, this is not the case outside the EU. There are countries with a high level of protection, countries with a different methodology of protection and countries with no protection of Privacy as a fundamental right.

7.4.1 The principles

Article 25, paragraph 1, of the Directive sets out the principle that Member States shall only allow a transfer to take place if the third country in question ensures an adequate level of protection.

Nevertheless, this general principle is flexibilised in different ways by the following provisions of the Directive.
The notion of « adequate » protection has to be linked to the degree of risk a transfer presents and to the nature of the data.

Article 25, paragraph 2 of the general Directive states: *« The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and*

sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country ».

7.4.2 Special derogations

There are some cases in which a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection can take place.
They are mentioned in article 26, paragraph 1.: *« (a) the data subject has given his consent unambiguously to the proposed transfer; or*
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party ; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.»

7.4.3 Commission's decisions of adequacy

Another possibility is to evaluate if the European Commission has passed a decision of adequacy concerning the country of destination of the data. Article 25, paragraph 6 foresees:
« The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. »
The European Commission has adopted, up to now, three Decisions under Article 25.6. The first one, concerning the US and known as "Safe Harbor"[34], determines that an arrangement

[34] Commission Decision of pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.

put in place by the US Department of Commerce provides adequate level of protection for personal data transferred from the EU. Decisions have been adopted also concerning Switzerland[35] and Hungary[36].

We will start by referring briefly to the decision concerning the US.

The US point of view differs deeply from the European one insofar the privacy Protection is considered as sufficiently ensured through self-regulation and not through a legislative approach considered as inadequate and costly by the US Government.

It was necessary to look for a solution to allow data flows from the EU to the US within a safe framework. The Commission has negotiated with the US Department of Commerce. The results are the Safe Habour principles, which are supplemented by FAQs (Frequently Asked Questions), published by the Department of Commerce and providing guidelines for the implementation of these principles.

Adherence to these principles by US companies is voluntarily. When subscribing to the principles, companies must reveal their confidentiality rules and fall within the competence of the Federal Trade Commission.

The Decisions concerning Switzerland and Hungary have a different approach since both countries have general Data Protection laws that have binding legal effect and both countries have ratified the Council of Europe Convention on the protection of Individuals with regard to Automatic Processing of Personal data (Convention nº 108).

http://europa.eu.int/comm/internal_market/en/dataprot/news/decision.pdf

[35] Commission Decision of 26 July 2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided in Switzerland. OJEC L 215, 25/08/2000.

[36] Commission Decision of 26 July 2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided in Hungary. OJEC L 215, 25/08/2000

7.4.4 Contractual Clauses

There is another alternative way for making a safe transfer mainly based on self-regulation. Article 26.2 prescribes : *« A Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses ».*

These appropriate contractual clauses can be proposed by the controller to the Member State Authority for approval, and can be accepted by this Authority.

Furthermore, the Commission can elaborate "Standard Contractual Clauses", as referred to in Article 26, paragraph 4: *"Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision."*
On 15 June 2001 the Commission has passed a Decision on Standard Contractual Clauses for the transfer of personal data to third countries under Directive 95/46/EC[37].
The Decision obliges member States to recognise that companies or organisations using such standard clauses in contracts concerning personal data transfers to countries outside the EU are offering "adequate protection".
Use of these standard contractual clauses will be voluntary but will offer companies and organisations means of complying with their obligation to ensure "adequate protection" for personal data transferred to countries outside the EU which have not been recognised by the Commission as providing adequate protection for such data. Data Protection Authorities in the Member States retain powers to prohibit or suspend data flows in exceptional circumstances.
The Decision refers to transfers made from a "controller"[38] who is established inside the EU to another "controller" who is established outside the EU.

[37] Available at http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf

[38] "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law." Article 2, paragraph d), Directive 95/46/EC

There is a Draft Decision on Standard Contractual Clauses[39] that regulates the transfers made from a "controller" located inside the EU and a "processor"[40] located outside the EU, dated 1st July 2001.

APPENDIX
GUIDANCE NOTE ON TRANSFERRING PERSONAL DATA ABROAD

The EU Data Protection Directive (95/46/EC) regulates the transfer of personal data to countries outside the European Economic Area (EEA). All types of data transfer potentially fall under the regulation, including for example the transfer of data within e-mails. It may also include the transfer of written or printed information. This note outlines the key considerations that should be borne in mind where, in the context of your activities, you intend to transfer personal data outside the EEA.

The general rule laid down by the Data Protection Directive is that personal data should not be transferred to a country outside the EEA unless that country has an *adequate* level of protection.

However, before addressing the question of what is 'adequate' protection, consideration should be given to whether this general rule applies to the type of transfer being envisaged. In the following circumstances, the general rule *may not apply*:

- The transfer is to another European Economic Area country, ie. to one of the European Union Member States, or Norway, Iceland and Liechtenstein. Note that Jersey, Guernsey and Isle of Man are *outside* of the EEA.
- The organisation to whom the data is transferred is merely processing the personal data under your instructions and control, and has no right to process the personal data on its own behalf or for anyone else (eg. an outsourced processing facility).

  Note: Where an entity is processing personal data under your instructions, the law requires that a contractual agreement be in place between the parties. The agreement should impose an obligation upon the data processor to implement appropriate technical and organisational security measures and to only process data on your instructions. A set of model clauses is attached at Appendix 2.
- The individuals who comprise the personal data have consented to the transfer. It is preferable if the express consent can be obtained and recorded; however, in certain circumstances it may be possible to imply such consent. In particular, it will be necessary to show that the individual was made aware that such a transfer was likely to take place, and has been given an opportunity to object to such a transfer.

[39] Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/sccprocessors.htm

[40] "'processor' *shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*". Article 2, paragraph e), Directive 95/46/EC

- The transfer may be necessary in order to enter into, or perform, a contract with the individual data subject, or with a third party, but at the request of, or in the interests of, the individual.
- An exemption from the 'adequacy' rule may also be possible where the transfer is in the vital interest of the data subject; the transfer is necessary or legally required on important public interest grounds, or in relation to a legal claim; or the transfer is from a public register. However, these are unlikely to be relevant to the types of transfer carried out within the normal course of business.

Note: If there is any doubt whether one of these exemptions applies to the transfer being envisaged, please contact your data protection officer, local legal counsel or the National Regulatory Authority.

- Finally, transitional provisions in national legislation implementing the Data Protection Directive may limit the application of the 'adequacy' rule to certain types of processing until October 2001.

Where the transfer does not fall under these exemptions, then the general rule will apply: the transfer can only take place to a country that has an adequate level of protection.
A consideration of what is 'adequate' will vary according to the circumstances of each specific transfer or set of transfers. However, factors that may be relevant include:

⇨ the nature of the data,
⇨ the purpose and duration of the proposed processing operation or operations,
⇨ the country of origin and country of final destination,
⇨ the rules of law, both general and sectoral, in force in the third country,
⇨ and the professional rules and security measures

Any determination of 'adequacy' *must* be appropriately documented and archived.
Certain countries may be considered to be adequate by virtue of laws in force in those countries that provide appropriate protection to the processing of personal data. In due course, national data protection authorities may publish a list of such countries that can be consulted.
A business may consider entering into a contractual agreement governing the transfer of personal data. Such an agreement should lay down some common principles of good practice that must be complied with, and contain enforcement provisions that can be enacted in the event of a breach.

Note: The attitude of national data protection authorities to the use of contractual agreements to establish 'adequacy' is uncertain. However, model agreements have been drafted by industry bodies and are currently under consideration at a national and EU level.

MODEL CLAUSES FOR DATA PROCESSING AGREEMENTS

Note: These provisions should only be used after consultation your local legal counsel as to their appropriateness in the particular circumstances.

1. Warranties of the data processor

The Data Processor warrants that it has in place appropriate technical and organisational measures against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and adequate security programs and procedures to ensure that unauthorised persons will not have access to the data processing equipment used to process the Personal Data, and that any persons it authorises to have access to the Personal Data will respect and maintain the confidentiality and security of the Personal Data.

2. Obligations of the data processor

The Data Processor shall:

2.1 do such actions as are necessary to ensure it has fulfilled, and will continue to fulfil, the warranty set out in Clause 4;

2.2 process the Personal Data in accordance with the Data Protection Act 1998;

2.3 shall process the Personal Data strictly in accordance with the instructions of the Data Controller [……]

2.4 shall comply with all instructions from the Data Controller to rectify, delete and update any Personal Data and shall confirm to the Data Controller within a reasonable time that it has done so;

2.5 appoint, and identify to the Data Controller, an individual within its organisation authorised to respond to enquiries from the Data Controller concerning its Processing of Personal Data;

2.6 submit its data processing facilities, data files and documentation needed for processing to auditing and/or certification by the Data Controller (or other duly qualified auditors of inspection authorities not reasonably objected to by the Data Processor and approved by the Data Controller to ascertain compliance with the warranties and undertakings in these Clauses); and

2.7 notify the Data Controller of any provisions in the law which do or could affect the Data Processor's ability to perform its obligations under these Clauses.

TIP

The Commission has published standard contractual clauses for the export of personal data and for the transfer to a third country for mere processing:

See http://www.europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/index.htm

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (CEDIB)
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON (CCLS)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

IST Project 1999 - 12278

Electronic Commerce Legal Issues Platform II

CHAPTER 8

Dispute Resolution Services for ISPs

3 CHAPTER 8

4 8. Dispute Resolution Services for ISPs

8.1 Objectives

The objective of this chapter is to describe different dispute resolution services for ISPs. These dispute resolution services use what is often referred to as alternative dispute resolution mechanisms (ADR), and represent an alternative to the dispute resolution system offered by traditional courts. When web- and computer based technologies are used for facilitating ADR, this is loosely referred to as online dispute resolution (ODR).
The purpose of using ADR can be to prevent disputes from arising. It can provide an incentive for the parties to settle before the need to formalise their problems with a third party. It can also ensure a fair, effective and meaningful redress without undue cost or burden.
It is important to stress that ADR services will not replace ordinary court procedures. Rather they supplement the traditional court system. The new ADR and ODR mechanisms that are being developed today also supplement the different ombudsmann schemes, consumer complaint boards, mediators and dispute settlement services already in place, offered by public bodies, trade associations, etc.
The European Union has taken several initiatives to promote ADR solutions in Europe. For instance, the European Commission has addressed the issue through Commission Recommendation 98/257/EC and the Communication from the Commission of 04.04.2001. Also, article 17(1) of the EC Directive on electronic commerce[41] requires the Member States to ensure that their legislation *does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means*. It follows from these initiatives that ADR and ODR solutions are seen as an important step in the process of improving confidence in e-commerce, and especially consumer confidence. OECD and Consumers International have in recent surveys identified more than 40 ODR mechanisms, and these will hopefully be important instruments in the further development of e-commerce.
This chapter will give an overview of the advantages and the need for ADR and ODR. The different principles that such dispute mechanisms should be based on will be discussed, and the different forms of ADR will be described. Finally, the legal framework for ADR will be covered, and some recommendations for e-businesses will be given.

8.2 Advantages Gained by Using ADR

ADR services are frequently used to solve disputes in different sectors, and represent an important instrument for both on-line and off-line businesses. Especially for e-commerce and international transactions there is a great need for ADR services, because the traditional court system is not always well suited to settle disputes that arise in such cases. There are several reasons for this. First of all, procedures before the traditional courts are expensive and time consuming. Also, the international character of e-commerce transactions can make it difficult to determine which court has competence to solve the dispute in question. If the parties to the disputes are situated in different countries, at least one of then must bear the expenses and

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

inconveniences associated with having the case tried in a foreign country. Finally, traditional courts are not specialised in legal issues relating to e-commerce. The disadvantages of the traditional court system are particularly apparent in disputes where consumers are involved. Most consumer disputes are by their very nature characterised by a imbalance between the economic value at stake and the cost of its judicial settlement. Also, the difficulties that court procedures may involve in cross-border conflicts will discourage consumers from exercising their rights in practice.

ADR and ODR offer the opportunity to solve the dispute fast and at a low cost. This is often one of the highest priorities for the parties. Also, the possibility of using specialised tribunals to solve the dispute can increase the chance of reaching a solution that is practical. A third advantage is that disputes can be solved in confidentiality, which is normally not the case for ordinary court hearings. Mediation can also maintain business relationships far more effectively than litigation. For international transactions, the parties can reduce the legal uncertainty involved in determining the competent court by agreeing to use ODR. In summary, ODR can reduce the inconveniences caused by the parties being domiciled or established in different countries.

ADR is not strictly restricted to solve disputes in the same way as ordinary courts. ADR includes different forms of negotiation, mediation, conciliation and arbitration. It can be used to prevent conflicts form developing as well as to help the parties to solve their conflicts through agreement. In this sense, ADR represents a much more flexible form of dispute resolution than the traditional court system. Some different forms of ADR will be described in the next section.

8.3 Different ADR mechanisms

ADR covers a variety of dispute resolution mechanisms offered by of out-of-court bodies, and can consist of everything from the most informal assisted negotiation, to formal and court-like binding arbitration.

Assisted negotiation and ***mediation*** is an informal and private collaborative process in which a professional third party assists the parties to reach an agreement. The third party does not decide on the conflict nor recommend solutions. However, he can help the parties communicate clearly, identify the key issues, search for common ground and develop solutions that are acceptable to the parties involved. Assisted negotiation and mediation always takes place on a voluntary basis. No party can be forced to participate, and either party may abandon the process at any stage before an agreement is reached.

The process can also be designed so that the third party plays a more active role. Even if the third party does not decide on the conflict, he can make recommendations and suggestions based upon what he sees as fair, or what he believes is legally correct. This is often referred to as ***conciliation***.

The disputing parties also have the opportunity of seeking an ***expert evaluation*** of their dispute. By doing this, the parties turn to a professional third party who can efficiently and effectively gather and assess claims and information, interview witnesses and provide an expert opinion on settlement. The evaluation can be based on law or on what the expert sees as fair. This decision does not have to be legally binding, but will give the parties guidance on how to settle.

Arbitration is a process in which the disputing parties present their evidence to a neutral arbitrator in a formal or informal setting. The arbitrator issues a decision that settles the conflict based on the presentations made by the parties. This decision can be based on law or fairness/equity, and can be binding or non-binding. This depends upon what the parties have agreed on beforehand. Once the parties have freely agreed to submit a dispute to binding arbitration, a party cannot unilaterally withdraw from the arbitration process.

These are just some forms of ADR, and there are others. Some of these are ***hybrid versions*** that combine the different processes described here. One option is to let the third party first act as a mediator, but also give him the power to make a binding judgement if no agreement is reached. It is up to the disputing parties to decide upon which form of ADR they wish to use, and the role of a third party that they may involve. It is therefore possible to design a process that meets their particular needs.

8.4 Important ADR Principles

In order for ADR to have good results, it is important that these mechanisms respect certain basic principles. Therefore, the Commission Recommendation 98/257/EC for binding procedures and also Council Recommendation 2001/310/EC[42] for non-binding procedures adopt a set of minimum principles for the operation of out-of-court procedures for resolving consumer disputes. These principles are of general interest, and will briefly be described here.

4.1.1 8.4.1 Independence

In order to guarantee the impartiality of the decision-making, it is important that it is independent of the disputing parties, and that it does not share common interests with any of them. This is necessary to ensure the parties' confidence in the process. Some ways to ensure the independence of the decision making body is to make sure that the person appointed possesses the abilities and experience required, is granted a period of office of sufficient duration, and is not directly remunerated by any of the parties. If the decision is taken by a collegiate body, the independence of the body responsible for taking the decision can be ensured by giving equal representation to consumers and professionals and by complying with the criteria mentioned above.

8.4.2 Transparency

Transparency is important to establish sufficient trust in the procedure. Transparency can be ensured by providing information such as the types of disputes that may be referred to the body concerned, as well as any existing restrictions in regard to territorial coverage and the value of the dispute. It is also important to inform the consumer about requirements that he may have to meet, the language of the procedure, the possible cost of the procedure, and the legal force of the decision taken. The Commission Recommendation also lists other types of information that should be provided.

8.4.3 Adversarial Principle

The procedure should allow the parties concerned to present their viewpoint before the competent body and to hear and respond to the arguments and facts put forward by the other party, and any experts' statements. This is a fundamental principle in ordinary court hearings, and should also be respected by ADR bodies.

8.4.4 Effectiveness

The effectiveness of the procedure is of great importance, and is one of the reasons for using ADR instead of settling disputes through the ordinary court system. Effectiveness can be ensured through measures guaranteeing that the consumer is not obliged to use a legal

[42] This Recommendation was issued by the European Commission on 4 April 2001 and is published in OJ L109 of 19. April 2001, p.56

representative, that the procedure is free of charge or of moderate cost, and that only short periods elapse between the referral of a matter and the decision.

8.4.5 Legality

The decision taken by the body may not deprive the consumer of protection afforded by mandatory provisions of law. In the case of cross-border disputes, the consumer must not be deprived the protection afforded by the law of the Member State in which he is normally resident in the instances provided for under international private law. All decisions should be communicated to the parties concerned as soon as possible, in writing or any other suitable form, and should state the grounds on which they are based.

8.4.6 Liberty

ADR can only be used if both parties have agreed to this in advance. Also, a decision taken by any third party is only binding on the parties if they were informed of its binding nature in advance and specifically accepted this. Consumers may not agree to ADR procedures prior to the materialisation of a dispute, where such commitment has the effect of depriving the consumer of his right to bring an action before the courts for the settlement of the dispute.

8.4.7 Representation

The procedure should not deprive the parties of the right to be represented or assisted by a third party at all stages of the procedure.

8.4.8 Common weaknesses

The international organisation Consumers International has conducted a study of different ADR mechanisms offered to consumers. The result of the study is that common weaknesses include limited availability (both in terms of merchants and language), high cost to consumers, failure to include adequate consumer representation on the governing board, lack of transparency (in terms of result records and officials' credentials), lack of scalability (adapting the service to the nature of the dispute), failure to accommodate cultural differences, and limited incentives for compliance with the verdict of the dispute resolution process.[43]

8.5 The Legal Framework

Art. 6 of the European Convention on Human Rights states that everyone should have effective access to the courts. This does not imply that parties involved in a dispute cannot choose to resolve their dispute out of court in an alternative way, provided that they both agree to do so. This is also the general rule in most national legal systems. The point of departure is therefore that the parties are free to agree on how their dispute should be solved, but there are certain limitations. These limitations will be examined here. It is not possible to examine the internal legal system in all the different Europeans states in this brochure. The analysis will therefore focus on legal limitations on a European level and on principles of common interest. It is also limited to a European context.

[43] The executive summary of the study can be found at http://www.consumersinternational.org/campaigns/index.html

8.5.1 General Legal Requirements

The first legal question is whether there are any legal requirements that an agreement to settle a dispute by using ADR must fulfil. The fact that the parties as a general rule are free to settle their disputes through out-of-court bodies does not necessarily mean that all such agreements are valid.

The main requirement is that in order to be valid the ADR agreement must be sufficiently clear and unambiguous. Also, a decision taken by third person or out-of-court body is binding on the parties only if they were informed of its binding nature in advance and specifically accepted this (binding arbitration).[44] The ADR agreement can be reached on an "ad hoc" basis after the dispute has arisen, or at an earlier stage. A typical situation is that the parties include a clause about dispute resolution in their original contract. If the ADR clause is included in general terms of contracts used by one of the parties, the validity of such a clause may be controversial, particularly if the other party is a consumer. Accordingly, such clauses should be carefully drafted. The main requirement is that the existence and content of the clause is made sufficiently clear to the other party.

There are no formal requirements on how agreements to settle disputes though ADR must be made. Article 9 of the EC Directive on electronic commerce requires the member states to ensure that their legal system allows contracts to be concluded by electronic means. This also includes ADR agreements, and means that agreements to settle through ADR are valid even if they are made electronically.[45]

The second question is if there are any legal requirements that the chosen form of ADR needs to fulfil. The general answer is that the parties are free to find the ADR mechanism that best meets their needs. However, article 17(2) of the EC Directive on electronic commerce states that the Member States are obliged to *encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.* This provision could be interpreted as to oblige Member States to guarantee the observance of certain procedural standards by ADR services. The interpretation of the clause is not clear, but it seems fair to say that the chosen ADR mechanism should comply with certain minimum standards. In any case it is not advisable for the parties to settle their disputes through ADR processes where certain minimum standards are not observed. For instance, the chosen ADR procedure should at least comply with some of the general principles stated above.

The third question is the legal effects of the outcome of the ADR process. The final result or decision can be either binding or non-binding. As stated earlier, in order for a decision made by a third party to be binding, the parties must agree on this ahead of time (binding arbitration). If such an agreement has been made, the next question is whether the decision is directly enforceable or not. Even if the ADR agreement is valid, and the process meets all necessary minimum requirements, this does not mean that the result is automatically and directly enforceable. For domestic disputes, the enforceability of the decision depends upon

---

[44] This principle is stated in principle VI of the Commission Recommendation 98/257/EC. Although the Recommendation is not legally binding, it is fair to assume that it only states a principle that can be found in most national legal systems in Europe.

[45] 1968 Brussels Convention on jurisdiction and the enforcement of judgements in civil and commercial matters dores not apply to arbitration, and therefore it does not stipulate any formal requirements that the ADR agreement has to meet. However it is worth mentioning that an electronic agreement on jurisdiction will probably be valid after the Brussels convention, even if the convention states that such agreements must be done *in writing*. This is particulary clear after the new *Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters* – which is largely identical to the Brussels Convention, and will replace this convention when it enters into force on 1 March 2002.

the requirements in national law. For international enforcement, the arbitration agreement and procedure must fulfil the requirements of the relevant international conventions on enforcement of international arbitral awards. The most important legal instrument regulating international arbitration is the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, New York 1958.[46] The Convention explicitly states several requirements that the arbitration process needs to fulfil in order to be directly enforceable. If the decision reached is not directly enforceable, it will be viewed as a contract agreement. Then the party that wants to enforce the settlement against the other party will normally have to institute legal proceedings based on a breach of contract. International mediation and/or conciliation is hardly regulated, taking into account that it does not follow a strict legal procedure and remains under the control of the parties. If the dispute is settled through negotiation or mediation, the agreement made by the parties will not be directly enforceable. The settlement will be viewed as contractual.

8.5.2 Consumer disputes

Up until now, arbitration has not played an important role in consumer disputes. However, it is seen as an important instrument in the future, especially in disputes relating to electronic commerce. The ADR initiatives taken by the European Union can be seen as a result of this view. The legal framework for consumer disputes is still not harmonised on a European level to any great extent. However, principle V of the Council Recommendation offers important guidance (principle of liberty, section 8.4.6 above).

In the same way as for non-consumers disputes, an ADR agreement is only binding on the consumer if the consumer specifically accepted it in advance. In order to be valid, the ADR clause must be sufficiently clear and unambiguous, and the consumer must be made aware of the clause before the contract is entered into. It is therefore of importance that the ADR clause is carefully drafted.

The Council Recommendation states that the consumer cannot agree to use ADR procedures prior to the materialisation of a dispute if the agreement deprives the consumer of his right to bring the dispute before the ordinary courts. The Council Recommendation is not legally binding, but similar principles can also be found elsewhere. A good example on the European level is Article 17 of the new EC Regulation on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters[47]. It states that consumers cannot, prior to a dispute has arisen, agree on a different jurisdiction than those indicated in the regulation, if this deprives the consumer of the right to bring the dispute before a court that would otherwise have jurisdiction to hear the case.[48] On the national level, the Norwegian Act on Consumers Right of Withdrawal from Distance Contracts[49] is another good example. Section 4 of the Act explicitly states that the consumer cannot make a prior commitment to settle disputes that may arise by arbitration. Also such a term, if not individually negotiated may be unfair under the Unfair Terms in Consumer Contracts Directive 93/13. Based on these different sources, it is fair to say that even if the Council Recommendation is not legally binding, it expresses a general legal trend which says that the consumer cannot make a prior commitment to use ADR mechanisms before the moment when a dispute has arisen.

[46] United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, New York 1958, (New York Convention), for the text of the Convention see http://www.uncitral.org/en-index.htm.

[47] Coucil Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters

[48] The same provision is also found in article 15 of the current 1968 Brussels Convention on jurisdiction and the enforcement of judgements in civil and commercial matters.

[49] Norwegian Act of 21 December 2000 number 105.

Even if the consumer cannot make a binding prior commitment to settle disputes through ADR mechanisms, the professional party can make a one-sided commitment that the consumer can choose to use ADR to settle disputes that might arise. By doing this, the professional party might increase the consumer's confidence and willingness to do business with him. Since lack of consumer trust is one of the main obstacles that electronic commerce faces today, it can be advisable for the professional party to do this.

8.6 Recommendations

The parties should consider if they wish to settle their disputes through ADR mechanisms. Depending on the type of dispute in question, different ADR schemes can have several advantages compared to the ordinary court system.
It is also advisable that the parties carefully consider which ADR scheme that best meets their particular needs. ADR can consist of a number of different methods to settle disputes, and they all have their advantages and disadvantages. For instance, the parties can choose an arbitration scheme that allows them to settle the conflict quickly, and to have the decision directly enforceable. On the other hand, they may wish to use mediation, since this might allow them to reach a more flexible solution. Reaching an agreement through mediation can also improve the parties' chances of having a good working relationship in the future.
If the parties wish to use an ADR or ODR service, they should be aware that there are several ADR and ODR service providers on the market. These services can be of varying quality, and they can be designed to meet different needs. It is therefore recommended that the parties consider some of the different services available before deciding on which one to use.
When should the ADR agreement be made? It will often be easier to reach an ADR agreement before a dispute has arisen than after. The parties should therefore consider whether to include an ADR clause in their original contract. It may, of course, in some cases be easier to determine which ADR scheme is appropriate after a dispute has materialised. However, even if the parties have made a prior agreement, the parties are free to reach a new ADR agreement at this stage.
As mentioned above, a consumer's agreement to settle disputes through ADR mechanisms that is made before the moment when a dispute has arisen, can be of questionable validity. However, the professional party can make one sided commitment to allow future disputes to be settled through ADR. On one hand, this is an extra burden for the professional party. On the other hand, it can be a sign of good will. Also, it can be a way to increase the consumer's confidence in the business, and therefore also his willingness to do business. Since lack of trust is one of the main factors that limit electronic commerce today, it is recommended that businesses consider if they should offer to settle disputes through ADR and ODR.

Some of the most important schemes:

BBBOnline	www.bbbonline.org
ECODIR	www.ecodir.org/
ClickNsettle	www.clicknsettle.com
Cybercourt	www.cybercourt.de
e-Mediator	www.consensus.uk.com
Squaretrade	www.squaretrade.com/cnt/jsp/index.jsp
e-Resolution	www.eresolution.ca
iCourthouse	www.i-courthouse.com

iLevel www.ilevel.com

Mediate.com http://www.mediate.com/

Internet Ombudsman www.ombudsman.at

NovaForum.com www.novaforum.com

Online Resolution www.onlineresolution.com

SettleOnline www.settleonline.com

WebAssured.com www.webassured.com

Web Trader www.which.net