

# Don't Panic! Do E-commerce

A Beginner's Guide to European  
Law Affecting E-commerce

**By Corinna Schulze and Jeffrey Baumgartner**

Published by the European Commission's  
Electronic Commerce Team  
(Information Society Directorate General)

© 2000, 2001 Corinna Schulze and Jeffrey Baumgartner

---

Disclaimer: the views expressed in this book are the authors' own and do not reflect the official view of the European Commission.

### **Acknowledgements**

The writers wish to thank  
Bror Salmelin, Ronald MacKay,  
David Benson and Sonia Luthra  
for their support and assistance in preparing this guide

**Don't Panic! Do E-commerce**  
*A Beginner's Guide to European Law  
Affecting E-commerce*

<b>Foreword</b>	<b>4</b>
<b>Introduction</b>	<b>6</b>
<b>1. The State of E-commerce in Europe</b>	<b>7</b>
<b>2. The Business Changes</b>	<b>10</b>
<b>3. E-commerce Law – Contracts</b>	<b>13</b>
<b>4. Jurisdiction</b>	<b>30</b>
<b>5. Cross-Border Alternative Dispute Resolution</b>	<b>34</b>
<b>6. Electronic Signatures</b>	<b>39</b>
<b>7. Payment Systems</b>	<b>43</b>
<b>8. Consumer Protection</b>	<b>46</b>
<b>9. Data Protection</b>	<b>49</b>
<b>10. Intellectual Property</b>	<b>53</b>
<b>11. Taxation and E-commerce</b>	<b>60</b>
<b>12. Liability of Intermediaries</b>	<b>66</b>
<b>13. And the Future...</b>	<b>67</b>

## Foreword

After a slow start, electronic commerce (e-commerce) is taking off in Europe. People are going on-line at unprecedented rates and on-line shops are popping up left and right. To see a business card without an e-mail address is becoming rarer and rarer these days. Nevertheless, there are still a number of barriers preventing many small and medium sized enterprises (SMEs) from going on-line and causing consumers to be wary of shopping on line. The law is one of them.

Many existing SMEs are confused by e-commerce-related law and so are reluctant to go on-line. They are often established companies that have been doing business for years, if not generations. But, their business has always been local. Suppliers are local. Customers are local. And, of course, the law is local. They know that when they put their business on the web, suppliers and customers could come from anywhere in the world – and that translates into a whole new set of laws to deal with.

At the same time, many new start ups are launched by young technicians and marketing people with innovative ideas, bags of venture capital and stacks of enthusiasm. They launch their businesses in complete ignorance of relevant law and, as such, are all too likely to run foul of it sooner or later.

This guide aims to be a beginner's guide to e-commerce law in Europe, pointing out the key relevant laws for e-businesses. It is important to bear in mind that this booklet does not even pretend to be a complete guide to legal issues. Moreover, just as the industry is moving at a phenomenal rate, so too (albeit slightly more slowly) is e-legislation. If you have questions, check with a legal professional or a completely up-to-date resource.

Finally, as our title says, "Don't Panic. Do E-commerce". Once a basic understanding is gained, it is clear the law is not that

complex. As you will see, a great deal is based on common sense. If you have that, you should not have any problems doing e-commerce – at least not from a legal perspective.

Good luck.

## Introduction

This guide is designed to give entrepreneurs and existing businesses an overview of European e-commerce legislation. It addresses key areas of legislation, how they affect business and ways that business might react to this legislation. In addition, this volume includes a number of "suggestions" which are generally based on a combination of legislation, best practice and the authors' experience.

E-commerce covers a wide range of activities, from selling books to consumers to selling container loads of supplies to factories across the globe. Companies are selling everything from physical goods, to services, to digital products delivered over the net. Clearly it would be impossible to cover every piece of legislation that might affect every e-commerce enterprise. However, this book does cover the legislation that affects most e-commerce activities and focuses on business to consumer (more trendily known as "B2C").

For the entrepreneur planning on launching a dot-com or the existing business planning on going from bricks-and-mortar to clicks-and-mortar (i.e. from selling out of a shop to selling both from a shop and via the web), it is essential to view their venture holistically. E-commerce is not just a matter of cutting edge technology. Rather, it is a combination of technology, marketing, legal circumstances and social impact. And it is those vendors who plan their venture and strategy with all these in mind who will best succeed in business.

Finally, it should be noted that this booklet does not reflect the official view of the European Commission. Rather it reflects the authors' understanding of European e-commerce legislation and e-commerce in general.

### 1. The State of E-commerce in Europe

E-commerce is growing by leaps and bounds. By 2003, the number of people buying on-line will have trebled and transactions will have increased in value twenty-fold. By this time, it is expected that Europe's on-line population will have exceeded America's and companies connected to the web will account for some 80% of the European GDP.

E-commerce has been broken down into all kinds of categories based on who is selling to whom. The focus has generally been on Business-to-Consumer (B2C) and Business-to-Business (B2B). However, there is also government to business, government to consumer and vice versa in both instances, as well as consumer to consumer and consumer to business.

### Definitions

There are many different formal definitions of *e-commerce* and *e-business*. For the purposes of this guide, e-commerce refers specifically to buying and selling products or services over the Internet. E-business refers to all aspects of doing business electronically. The E-commerce Directive cited many times in this guide refers to *information society services*. For the purposes of this guide, information society services can be considered e-business.

As is clear from their names, B2B is a business selling to other businesses while B2C is a business selling to consumers. B2B exploits Internet technologies to re-engineer processes along the organisation's value chain in order to lower costs, improve efficiency and productivity, shorten lead times, and provide better customer services.

B2C e-commerce does not present such clear improvements in the value chain, but has certainly received the lion's share of attention. B2C widens a business's potential market to include much of the world and has the potential to provide convenience

to consumers, particularly those not near shopping centres. Much has been said about consumers benefiting by being able to research and buy from the merchant offering the best price, but research indicates that this is not happening to the extent expected. It is likely that consumers are also looking for added value, merchants they can trust and proximity (to ensure prompt delivery of their purchase).

The European Union and Member States have been supporting e-commerce for years through a variety of means from developing a legislative framework to providing funding for research and development. Governments have also supported awareness-raising initiatives, training schemes and other pro-e-commerce activities.

## **eEurope**

*eEurope* is an initiative which aims to get everyone in Europe – every citizen, every school, every company – on-line as quickly as possible. The *eEurope* initiative builds on the current policy framework, concentrating on priority actions to overcome handicaps in Europe that are holding back the rapid uptake of digital technologies. *eEurope* actions are:

1. European youth into digital age
2. Cheaper Internet access
3. Fast Internet for researchers and students
4. Smart cards for secure electronic access
5. Risk capital for high-tech SME's
6. eParticipation for the disabled
7. Healthcare online
8. Intelligent transport
9. Government on-line
10. Digital content for a global network

A key barrier to the take up of Internet use in Europe has been comparatively expensive telecommunications costs established

by state-owned telecommunications services. Therefore, the European Commission has taken the initiative to liberate the market for telecommunications infrastructures and services in the European Union as of 1 January 1998. Today there are 900 telecommunications enterprises on the European market. The prices for long distance calls have decreased in most European markets by 40 %. In many countries, the consumer can gain Internet access via a TV cable. Technological change will continue to make connecting to the Internet even easier. Faster home connections and mobile access to the Internet will vastly improve web site access.

Europe has a leading role in mobile communications and digital TV, both of which are user-friendlier to the non-technical person than a PC. Mobile phone ownership and use is high in Europe. In 1999 there were 140 million mobile phones in use (compared to 80 million in the US). If mobile devices connecting to the Internet and the infrastructure are fit enough, the number of "internauts" in Europe could increase from 50 million today, to 130 million in the year 2003. For the time being, however, the costs for Internet surfing via mobile phone are too high. As a result, the Commission has started another competition-sector specific campaign against roaming prices as well as for local telephone tariffs, which are still monopolised in many countries.

## 2. The Business Changes

### **An e-marketplace is not just a bazaar for parts and products**

E-marketplaces allow for instant communications throughout the supply chain giving the partners a clear real-time picture of supply and demand. Suppliers can now organise their production according to the needs of the customer. Producers can check online the availability of raw materials or where in the world an expected delivery is. In short, e-commerce uses information to cut down the need for inventory. Producers build each computer only when a customer has ordered it.

E-commerce creates revenue streams, saves costs, and enables businesses to better manage their inventory. Traditional business is governed by complex processes, and constrained by informational inefficiencies, geography and market hours. The Internet simplifies traditional business, facilitating a single destination for commerce, content, and community. The benefits of e-commerce for SMEs can include cutting costs, saving time, reducing inventory and making electronic repetitive processes that used to be handled manually and individually (such as writing up invoices, checking inventory, entering customer names on to mailing lists, etc).

Moreover, e-commerce can put customer information directly into a database, allowing businesses to better monitor customer behaviour, market to each customer individually based on their buying habits and react more quickly to trends. And much of this can be done entirely automatically using data-mining software.

In terms of purchasing, companies can tap into a global supply base and find the best value for their needs. They can bid at electronic auctions, invite offers on their own web sites and search the web for new suppliers. On-line discussion forums

allow businesses to share information with other businesses around the globe and thus to develop relationships that would not have been possible a decade ago.

## **Doing E-commerce**

Launching an e-commerce venture can range from putting a catalogue on-line in an established electronic shopping mall to developing an individual on-line presence with custom built tools to meet the vendor's specific needs as well as his customers'. On-line shopping malls are the least expensive and most painless, there are many of them and most of them provide "wizards" (electronic helpers) and simple tools that allow even the completely inexperienced to put together their e-shop in a matter of hours. Many of these services also provide payment services, tips and marketing support and generally costs are quite low – often less than €100 per month. Such businesses can be considered the high street shops of the Internet.

For the entrepreneur who thinks big, only an individual web presence will do. This requires hiring professionals to develop an e-commerce web site, the purchase, customisation and integration of sophisticated software, and substantial marketing budgets. The investments can be substantial – but so too can be the rewards. Fortunately, for the entrepreneur with a better idea than bank balance, venture capital can provide financial support and partnering can reduce costs.

Regardless of which path the entrepreneur chooses, once he is on-line there is a legal and regulatory framework that must be dealt with. Fortunately, it sounds more frightening than it actually is and, in many respects, following the law results in better treatment of customers. This is a good thing. Many potential e-commerce customers still lack trust and confidence in e-businesses, and existing e-commerce customers are regularly frustrated by on-line shops where they cannot find information

or which do not make processes clear. Hence, following the law can result in improved sales and improved customer relations. And that is not a bad thing.

### 3. E-commerce Law - Contracts

**Golden Rule**

The golden rule of complying with e-commerce law is:

**be transparent!**

By being completely and fully transparent about who you are, what you are doing and how you will serve your customer, you will find you are not only staying on the right side of the law, but you are also keeping your customers happy. Survey after survey has shown that customers are not happy with their e-commerce experience owing to lack of information. If you are generous with information, this will not be a problem. And in view of high customer acquisition costs on the web, it only makes sense to keep your customers happy.

The law in the field of e-commerce is continuously developing and fast moving, as numerous drafts pass into the statute books. The evolution of technology also means that legislation must be updated and requires constant review. Companies and individuals need to be aware of both the current and the prospective impact of legal provisions.

The EU is also developing law for e-commerce and (despite what many people think) the European Commission is trying to make life easier for small business. The Commission is working towards developing a common legal framework across Europe, referring to the freedom of circulation.

The purpose of EU law (which harmonises the differences between national laws) is to achieve the maximum opportunities for free trade. It is therefore critical for any organisation, trading or otherwise operating in the EU, to be aware of current and

prospective European law. While national law and EU law are mutually dependent, EU law takes precedence over national law.

For the purposes of this guide, *directives* are the most common form of European legislation. Directives are essentially instructions to the Member States to introduce legislation. Directives indicate the goals to be achieved, but do not lay down the manner of achieving them. In general, enforcement measures and remedies are left to the Member States. On average, Member States have two years from the date of publication of a Directive to transform it into national law. E-commerce regulation is teamwork between harmonised EU Regulatory Framework and national rules.

### **The Electronic Commerce Directive**

The EU Directive on e-commerce ensures that *Information Society services* – which for the purposes of this guide can be considered *e-business* (a legal definition of “information society services” can be found in Directive 98/48/EC; laying down a procedure for the provision of information in the field of technical standards and regulations) – benefit from the Internal Market principles of free movement of services and freedom of establishment. Generally speaking, information society services can be provided throughout the European Union (EU) if they comply with the laws in their home Member State. The E-commerce Directive establishes rules in areas including: definition of where operators are established; transparency obligations for operators; transparency requirements for commercial communications; conclusion and validity of electronic contracts; liability of Internet intermediaries; and on-line dispute settlement.

According to the E-commerce Directive, Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Only for the following categories can Member States provide that the contracts cannot be concluded by electronic means:

- contracts that create or transfer rights in real estate (except rental);
- contracts governed by family of succession law;
- contracts requiring the involvement of courts or public authorities;
- contracts requiring “surety and collateral securities” supplied by persons acting for non-professional reasons.

The E-commerce Directive covers all forms of e-business, including business-to-business (B2B) and business-to-consumer (B2C). Examples of sectors and activities covered include on-line newspapers, on-line databases, on-line financial services, on-line professional services (such as lawyers, doctors, accountants, estate agents), on-line entertainment services such as video on demand, on-line direct marketing and advertising and services providing access to the World Wide Web.

The E-commerce Directive will not apply to services supplied by service providers established in a third country (i.e. not in the European Union). It aims to be consistent with relevant international rules and discussions within international organisations (World Trade Organisation, Organisation for Economic and Commercial Development, UNCITRAL).

### **Which Law is Applicable?**

One of the big questions raised by e-commerce is, “which law is applicable?” When small companies sold goods or services from an outlet in a single country, this was not a question. Even mail order generally avoided raising this question.

The E-commerce Directive provides that information society service providers (ISSPs) are subject to the law of the Member State in which they are established (the so-called country of origin principle). As long as ISSPs comply with this law, they are free to pursue their activities throughout the community. Certain

areas are excluded from the application of the principle of the country of origin because some existing directives require the application of the law of the country of destination, or because the mutual recognition principle cannot be achieved and there is not sufficient harmonisation to guarantee an equivalent level of protection throughout the Community (see section below). These directives relate, for example, to contractual obligations concerning consumer contracts, copyright, related rights and industrial property rights, and permissibility of unsolicited commercial communications by e-mail.

## **B2B Contracts**

National laws govern the main aspects of contract law. Laws governing the constitution of a contract and the point at which a contract is concluded currently vary from country to country. An offer of a product may be a binding offer in one country but not in another. In general, a contract is governed by the law chosen by the parties to the contract in what is called "private autonomy". It is advisable to make a clear choice of law in order to provide certainty for both parties.

In practice suppliers favour the application of their own national legislation for all contracts conducted on their web site (or other e-commerce platforms). The rules of international private law almost ensure that the laws of the supplier's nation will govern the contract made on his e-commerce platform. Provided the parties explicitly agree upon a governing law in their contract, their choice will be binding.

E-business managers may be surprised to know their web sites and e-mails contain invitations – even if not intentionally put there – to make a contract. Their web pages hold a description of products or services and a set of "self-contracting" pages that enable the web visitor to request these products or services.

How can the supplier explicitly agree upon a governing law in a contract? Firstly, he should inform his customers of his organisation's identity, place of establishment, domicile and trading status.

The E-commerce Directive provides that, except when otherwise agreed and except for contracts concluded exclusively by exchange of e-mail messages, the service provider should communicate "comprehensibly and unambiguously" prior to the placement of the order, at least the following information:

- the different technical steps needed to conclude the contract;
- the language available for the conclusion of the contract;
- the technical means for identifying and correcting input errors;
- whether the contract will be archived and be accessible.

In addition, the service provider must provide the recipient with the contract terms and general conditions in a way that allows him to store and reproduce them (e.g. by e-mail). Finally, except when otherwise agreed, the service provider must indicate any relevant codes of conduct to which he subscribes and information on how such codes can be electronically consulted. In the case of electronic transactions, care should be taken that both buyer and seller understand where the contract is accepted. If the vendor is located in Germany and the buyer in Italy or the buyer is on the move, which law governs the contract?

The supplier should incorporate on his web site an explicit clause of the applicable law. If the other contracting party accepts this clause, it will govern the contractual obligations of the parties based on the principle of party autonomy. The clause can be on the mandatory page (a page through which the purchaser must pass) and also in the general terms.

When the parties to the contract have not chosen the law applicable to a contract, the governing law is that of the country with which it is most closely connected. In almost all cases, a

B2B contract is most closely connected with the country of the establishment of the provider of the product or service. Under the EU Directive on e-commerce, the place at which an e-business is established should be determined in accordance with the case law of the Court of Justice. It recognises that the place of establishment of a company providing services via an Internet web site is not necessarily the place at which the technology supporting its web site is located or where its web site is accessible. Usually, the place of establishment is the place where the business is legally registered. In the case of multiple establishments, the competent Member State will be the one in which the supplier has the centre of his activities.

## Consumer Contracts

According to the Rome Convention, specific rules are applicable to certain consumer contracts. These are contracts for the supply of goods or services to a consumer provided that one of the following conditions are met:

- the consumer has received in his home state a specific invitation addressed to him, or by advertising, prior to the conclusion of the contract and he takes, in his home state, all the necessary steps to conclude the contract;
- the supplier has received the consumer's order in the country where the consumer is domiciled;
- the consumer travelled from his country to another one where he gave his order to buy a good, provided that the consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy.

Parties to these consumer contracts can choose the applicable law, **but** this choice *shall not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence*. Mandatory rules cannot

be limited or excluded by contractual provision. They will apply even if a contract states they do not. In particular, contracting parties cannot, whilst agreeing to be bound by the laws of a particular country, opt-out of the mandatory consumer protection provisions of that country. When contracts (whether in hard copy or electronic form) are being drawn up, it is important to state which is the governing law; and critical to ensure that the clause in which the governing law is specifically stated is within an electronic contract.

Mandatory rules are laid down in the Distance Selling Directive, the E-commerce Directive and by national law.

According to the Distance Selling Directive, the supplier must provide the consumer with clear and comprehensible information concerning:

- the identity and the address of the supplier;
- the characteristics of the goods or services and their price;
- delivery costs; delivery times;
- details of terms for returning goods;
- details of deadlines for returning goods;
- general terms and conditions of business;
- the arrangements for payment, delivery or performance;
- the existence of a right of withdrawal;
- the period for which the offer or the price remains valid and the minimum duration of the contract, where applicable;
- the cost of using the means of distance communication;
- and where appropriate the minimum duration of the contract in the case of permanent or recurrent performance.

The consumer must receive written confirmation or confirmation in another durable medium at the time of performance of the contract. The following information must also be given in writing:

- arrangements for exercising the right of withdrawal;
- place to which the consumer may address complaints;
- information relating to after-sales service;
- conditions under which the contract may be rescinded

This information must comply with the principles of good faith in commercial transactions and the principles governing the protection of minors. In the case of telephone calls, the caller's identity and commercial purpose must be made clear at the beginning of the call.

The E-commerce Directive provides that, except for contracts concluded exclusively by exchange of e-mail messages, the service provider should communicate "comprehensibly and unambiguously prior to the order being placed", at least the following information:

- the different technical steps needed to conclude the contract;
- the language available for the conclusion of the contract;
- the technical means for identifying and correcting input errors;
- whether the contract will be archived and be accessible.

The service provider must provide the consumer with the contract terms and general conditions in a way that allows storage and copying (e.g. by e-mail). He must also communicate any relevant codes of conduct and information on how such codes can be consulted on-line.

National legislation can contain general information requirements for the provision of information society services.

In the absence of a choice of law under a contract, the governing law is that of the country in which the consumer normally lives. This means that – in cases where no law was chosen – suppliers are subject to, and are best advised to be aware of, the national laws of 15 different EU member States.

**Suggestion**

Make it crystal clear on your web site where your business is located, which law is applicable (typically your own law), and provide the consumer with all the necessary information mentioned above. The way to do this is to ensure all main entry and informational pages on your site include your company's location. You should also clarify, on the page where your customer clicks to make a purchase, that the sale is subject to the laws of [your country]. The number of web sites that seem to hide their physical whereabouts is amazing!

Written confirmation or confirmation in another durable medium includes confirmation directly transmitted (e.g. by e-mail) onto the hard disk of a computer. Looking further into the future, there is no clarity about confirmation via WAP or other developing technologies. For example, what happens if a connection is cut during a transaction?

**Steps to Conclude a Contract**

According to most legal systems, three elements must be present for a contract to be formed – and normally a sale closed:

1. an offer from the seller to the buyer;
2. its acceptance by the buyer;
3. the E-commerce Directive specifies that the seller has to acknowledge the receipt of the buyer's order without undue delay and by electronic means.

Currently, the electronic catalogue on an e-commerce platform is not a real, definitive contractual offer, and therefore not immediately binding upon the supplier. The first contractual act is an offer made by the purchaser. The supplier will still be able to check the relevant personal data of the purchaser. The supplier can accept the offer by generating a confirmation of sale page, sending a confirmation e-mail or just by delivering the product or service.

The vendor is obligated to indicate the different technical steps that must be taken to conclude a contract. The consumer must be able, before concluding the purchase, to identify and correct any errors in the order, modify the order, consent to the purchase, and retain a complete accurate record of the transaction. The languages offered for the conclusion of the contract must be clear (see mandatory rules for the Distance Selling Directive; p. 20-21).

Community legislation does not specify at what time an electronic contract is deemed to be concluded. It is therefore determined by reference to Member States' laws. The E-commerce Directive provides for consumer contracts that:

- the service provider must acknowledge receipt of an order electronically and without undue delay; and
- technical means to identify and correct input errors prior to the placement of the order must be available.

**Suggestion**

When a customer in your e-shop completes his order and clicks on the "proceed to checkout" button, give him a preliminary receipt with all items purchased, their cost and any optional features (such as colour, size, etc). Have tick boxes and fields so he can change his order without having to cancel the entire order. Every time he makes a change, give him a new preliminary receipt. Make it clear that this is a preliminary receipt and he must still click on the "Buy" button to finalise his order (amazingly, a large number of people leave e-commerce sites at the preliminary receipt stage thinking they *have already completed the purchase* – so it is critical to ensure the customer understands at what point the order is made and at what point it is not.)

Once the customer clicks on the "Buy" button to finalise his order, you should immediately send him a follow up receipt via e-mail. This ensures your customer has a receipt (many will neglect to print or save the receipt page on their browsers). It is also a last chance to clear up any misunderstanding *before* you ship the products.

Some of the information to be provided before the conclusion of the contract (see box above) and other elements (i.e. the address to which complaints can be addressed, information on after-sales services and guarantees, conditions and procedures for exercising the right of withdrawal), must be communicated to the consumer in writing or in another durable medium such as by electronic mail. This must be done in good time during the performance of a contract and, for goods, at the time of delivery at the latest.

**Case Study**

Gizmo electronics has some E-733 computers that it intends to put on sale for just 999 Euro. Unfortunately, their web master is new and accidentally advertises on the web site: "Gizmo E-733 computers marked down to just 9.99 Euro until 31 August!" He also sends the same message on an e-mail to 100 of the company's best customers.

Within a day, dozens of orders have come in and Gizmo's marketing manager realises there has been a terrible mistake. He pulls the web page down and stops any more e-mail promotions being sent. Legally, how does he stand?

Orders from the web page, provided he has not acknowledged them, are not binding. Remember, a web page with an offer is an invitation to make a contract, but not a contract.

E-mails, however, are contracts. And once a customer has acknowledged his desire to accept the contract, Gizmo is legally obliged to fulfil the order at the rate offered in the e-mail.

This, however, ignores the issue of customer relations as recent similar cases have shown. And it is arguable that the cost of filling those dozens of loss-making orders would generate substantial positive publicity while refusing them would generate negative publicity.

## **General Terms**

Terms of trading should be incorporated into any contract between the buyer and seller, even if the terms are also on the relevant web site. National laws regulating contracts currently require that the general terms be made available to purchasers at the time of concluding the contract.

The general terms should be directly available to a customer when he makes an electronic purchase. This can be done, for example, by presenting the purchaser, when he concludes his order, with a web page of the general terms and an "Agree" button he must click to finalise the order. In addition to this, an explicit reference or hyperlink to the general terms can be made on the purchase order form. Moreover, it is advisable to have the general terms easily accessible (i.e. a minimum number of clicks away) from anywhere in the web site. The customer browsing an e-commerce site for fun may well decide to make a purchase. Allowing him to access general terms readily will only encourage that purchase.

General terms must be clear, easily readable and clearly arranged with regard to contents. As mentioned previously, the general terms can incorporate a clause stating which country's law will govern the contract.

The EU Directive on Unfair Contract Terms applies also to on-line contracts. It covers all contracts concluded between a seller or a supplier and a consumer for the supply of goods and services, but only the contractual terms that have not been individually negotiated (i.e. only standard contracts). It forbids any clause in a contract that creates a significant imbalance in the party's rights and obligations to the detriment of the consumer.

### **Right of Withdrawal**

The Distance Selling Directive states that the consumer has the possibility of withdrawal from the contract without reason or penalty (except for the direct cost of returning the goods i.e. postage). In the case where the supplier has met his obligations regarding the provision of information, the consumer has at least seven working days (depending on national regulations) to cancel the contract:

- for goods, from the day when the consumer has received the written confirmation or the information
- for services, from the day of the conclusion of the contract or from the day of the written confirmation of the information (where this confirmation occurred after the conclusion of the contract).

In the case where the supplier has failed to meet his obligations to inform the consumer about his rights, this period is extended to three months. The directive, which is only applicable to consumer contracts, requires that the supplier repay the money paid by the consumer within thirty days of cancellation.

Where the consumer exercises his right of withdrawal, the supplier must reimburse the sums paid free of charge within 30 days. Similarly, credit agreements aimed at ensuring the payment of the contract involved must be cancelled without penalty.

It should be noted that in some cases the consumer cannot exercise his right of withdrawal for products such as the supply of newspapers, unsealed audio or video recording or computer programs, periodicals and magazines.

In principle, the supplier has thirty days in which to perform the contract. Where the supplier fails to perform his side of the contract, the consumer must be informed and any sums paid refunded. In some cases, it is possible to supply an equivalent good or service. The possibility must be provided for in advance of the conclusion of the contract or it must be mentioned in the contract in a clear and comprehensible way.

The Distance Selling Directive also provides that if a consumer's payment card has been used fraudulently for a distant contract, the consumer must be able to:

- request cancellation of the payment;

- be credited with the sums paid.

### **Suggestion**

Since you are legally obliged to cancel an order and refund the consumers money if the consumer is not satisfied, why not use this as a marketing tool in the form of a money back guarantee?

**If you are not completely satisfied with our product, return it within seven days and we'll give you a complete refund – no questions asked!**

### **Written Requirements**

According to the E-Commerce directive, all Member States will have to remove any legal obstacle that could hamper the use of electronic contracts. The Electronic Signature Directive (Directive 1999/93/EC of December 13, 1999 on a Community Framework for electronic signatures) provides that electronic signatures cannot be denied legal effect (for the validity of contracts and as evidence in court) solely on the basis that they are in electronic format. Most Member States have already recognised the equivalence between electronic signatures and hand-written signatures and the admissibility of electronic signatures as evidence in court proceedings.

Contracts may be concluded orally but in practice they are written down to avoid misunderstandings. The reason is one of evidence and sometimes validity of the contract. If one country's national legal regulation requires a written form or a similar formality, an electronic contract is not valid. Another country's national law may only require written requirements in specific

cases, such as agency contracts, where one party requests a written contract, or real estate sales.

The implementation of the Directive on a Common Framework for electronic signatures and certification service providers will change the validity of electronic contracts concerning formal issues. Electronic signatures accompanied by a valid certificate will have equivalent validity to hand-written signatures throughout the EU, thus removing problems caused by varying national laws regarding the validity of electronic signatures.

## 4. Jurisdiction

### **Evidence Issues**

National procedural laws have been or soon will be adapted to allow the presentation of electronic documents. Evidence of the existence of an electronic contract may be produced by a digitally signed acceptance, but also after the fact through significant actions of the acceptant, such as making an ordering payment or accepting delivery of the purchased products. Digitally signed acceptances and other significant actions of the acceptant give evidence of the existence of a contract and its main elements. This does not cover other aspects of the contract, such as the general terms, fulfilment of the duty to inform, product features, or the presentation by the e-commerce platform.

One method of guaranteeing the evidence that the e-commerce platform was established in a particular version would be to permit a third party (a notary or other trusted third party) to periodically check whether the e-commerce platform that is functioning is the one previously set up by the e-supplier.

### **Which Courts Have Jurisdiction?**

Jurisdiction determines whether a court (or, typically for public law, a government agency) may hear and decide a case. The rules, for when a national court will have jurisdiction, are mainly a matter for national law to decide. The Brussels and Lugano Conventions determine the court before it has a "trans-border nature".

As a general principle, the Brussels Convention lays down that, in the absence of a specific rule, a court action must be brought before the court of the Member State where the defendant is domiciled. Nevertheless the parties to a contract, other than an

employment, insurance or consumer contract, are free to designate the court before which a case should be brought. Indeed, sellers are advised to express an exclusive jurisdiction on their web sites and in their contracts in order to avoid any confusion. Moreover, web site owners should make sure that their preferences regarding applicable law and choice of jurisdiction are in fact both valid and enforceable. For this it must be clear where the contract is formed. Both applicable law and choice of jurisdiction should be made clear to purchasers well before a contract is concluded, and on the web site itself.

### **Suggestion**

Jurisdiction can be a thorny issue, particularly in a cross border electronic transaction and especially when consumers are involved. This situation will become even more complex once mobile Internet becomes commonplace. For B2B contracts, to avoid troubles, make it perfectly clear on your web site that in the event of a dispute, jurisdiction is in your country.

Moreover, you should ensure it is clear to visitors where you are located. Making it clear can only help promote good customer relations. Surprisingly, a lot of e-businesses seem ashamed of their location as it can be difficult to determine from many web sites.

Again, there are specific rules applicable to contracts for the supply of goods or services to a consumer provided that one of the following conditions are met:

- the consumer has received in his home state a specific invitation addressed to him by advertising before the conclusion of the contract and he takes, in his home state, all the necessary steps to conclude the contract;

- the supplier has received the consumer's order in the country where the consumer is domiciled;
- the consumer travelled from his country to another one where he gave his order to buy a good, provided that the consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy.

Parties to these particular contracts can contractually designate a competent court under certain well-defined conditions:

- a clause must have been entered into after the dispute has arisen; or
- the consumer is allowed to bring proceedings in courts other than those located in his country or the defendant's; or
- the courts of the same country where the consumer and the supplier are located are designated.

In the absence of a contractual choice, the rules vary according to who initiates the proceedings:

- the consumer can either bring a court action before the courts of the country where the defendant is domiciled or before the court of the country of his own domicile;
- the supplier of goods and services on the other hand can only bring proceedings against a consumer before the courts of the Member State where the consumer is domiciled.

The relevant law for jurisdiction, the Brussels Convention, is now proving to be insufficiently precise to comprehensively cover the e-commerce environment.

In December 2000, the Council of the European Union adopted a Regulation "on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters" which will replace the Brussels and Lugano Conventions. The

Regulation takes into account new forms of commerce such as electronic commerce. Once in force on 1 March 2000, it will provide rules for determining the competent court in cases of transnational disputes, including e-commerce transactions within the European Union.

The Regulation, which is applicable whenever the defendant is domiciled in a Member State, provides a special regulation for contractual claims involving consumers. It states that a consumer could decide to sue a supplier before the courts of his own Member State whenever the supplier "has directed his activities" towards the consumer's Member State. This means that sellers will have to face proceedings in any of the EU Member States if they do not implement a disclaimer on their website to exclude certain countries. But don't panic! In any event, alternative dispute resolution (see next section) and other solutions are becoming available.

Full details of this complex issue can be found in the Regulation on jurisdiction, recognition and enforcement of judgements in civil and commercial matters.

## 4. Cross-Border Alternative Dispute Resolution

### **How to Avoid Disputes**

Most disputes are due to misunderstandings. Products don't meet expectations. Conditions are not clear. The method of fulfilment is not what was expected. These misunderstandings can be avoided by transparency and playing by the rules, as well as monitoring customer behaviour and collecting feedback. An extensive after-sales service (see also 3. Contracts) can also go a long way towards preventing problems.

#### **Suggestion**

Make sure it is easy to get e-mail and telephone contact information from your web site. Virtually every web user has experienced the frustration of trying to contact the owners of a commercial web site, only to find nothing, find a US based toll-free number or completely irrelevant e-mail links such as "investor relations". If your customers are annoyed already and have to spend a half-hour figuring out how to contact you, they will be irate when they actually make the complaint.

Of course having a contact point for complaints is not enough. It is critical that you respond to complaints as quickly as possible. Ignoring complaints is a great way to lose customers. Acting quickly and surprising annoyed customers with fast solutions, on the other hand, is a great way to retain customers. And remember: you need your customer's loyalty.

If complaints do arise, a clear and comprehensive refund policy will help, particularly if it is easily found at the time of ordering.

Having a clear complaints procedure together with contact points for complaints is also critical (see box below).

**Checklist**

You will avoid disputes if you ensure the following information is clearly stated and readily available on your web site (include a link on your main menu bar):

- conditions and procedures for exercising the right of withdrawal
- information on after-sales services and guarantees which exist
- conditions for cancelling the contract
- information on the way and the period of performance of the contract
- cancellation terms
- order fulfilment
- delivery times/costs

### **Different Types of Alternative Dispute Resolution (ADR)**

Of course it is impossible to avoid disputes, particularly in a new industry where the rules are being established and on-line trading provides opportunities for fraudulent, misleading and unfair commercial conduct both in B2B and B2C.

The problems involved in seeking redress from disputes over on-line transactions cannot be underestimated. The costs and the delays involved in litigation, particularly for consumers and SMEs, can be prohibitive and soon eclipse the value of the disputed product or service. The problems are compounded when the dispute is cross-border. The costs are higher, the delays are longer, and the relevance and effectiveness of the courts for resolving such disputes, especially when the value of the disputed product is low, is not obvious.

Uncertainty over the legal framework may not only inhibit consumers from purchasing products or services over the Internet, but also discourage companies from entering into the electronic market place.

Clearly, a means of solving disputes which includes the authority of the court but not the cost or inconvenience would be welcomed. Fortunately, it exists already. Alternative dispute resolution (ADR), which relates to all types of dispute settlement which are not litigated before a court, can solve complaints quickly and cheaply through arbitration or mediation by a trusted third party. Consumers, SMEs and business benefit from such systems by avoiding costly, time-consuming lawsuits in a legally fragmented and uncertain environment.

For international B2C e-commerce, characterised by a large volume of relatively low value transactions carried out across borders, the relevance and effectiveness of courts for resolving problems may be limited. Here ADR will likely prove to be the most popular and appropriate solution. Recent initiatives, from

the EU as well as at the global level, aim to develop ADR systems in order to create trust in e-commerce.

Private, public or non-profit organisations could all offer ADR services. Consumer organisations, trade and industry associations, public administrations or other "neutral" organisations may offer schemes through which out-of-court dispute settlements of consumer complaints can be dealt with. The most common ADR providers are often referred to as ombudsmen or consumer complaint boards.

Clearly, it is very much in the market's interest to develop ADR systems to provide confidence for business and consumers alike.

**Case Study from the Near Future**

Sylvia, who lives in Madrid, orders a set of coffee mugs, with her children's pictures and names on them, from YourMugs, an Irish firm. A couple of weeks after they have been delivered, she notices that the names have been spelled incorrectly. She complains to the company and demands a refund. They inform her that by company policy, which is published on their web site, they cannot refund money on customised products, unless they are informed within seven days of receipt of goods.

Sylvia refuses to accept this – the company made a clear mistake in misspelling one of her children's names. Going to court is out of the question for goods costing just 50 Euro. Then she notices the company belongs to eADR – an electronic alternative dispute resolution service.

She goes to their web site, pays 20 Euro to have a dispute judged (YourMug pays an annual subscription fee), enters her complaint, forwards relevant e-mails and waits. Two weeks later, eADR brings her bad news. Based on their published refund policy, the company is within the law and has no legal obligation to refund Sylvia.

*However, from a customer relations point of view YourMugs is certainly losing more value from a lost customer and the complaints she will doubtless make to friends, family and colleagues than would be lost by sending her a replacement set!*

## 6. Electronic Signatures

The anonymity and the openness of the Internet pose several questions for business.

- How can you be sure that the person you are communicating with is who he claims to be?
- How can you make sure that the communication cannot be changed at some time between transmission and receipt (with text-based e-mail, it is technically quite simple to change the content of an e-mail)?
- How can you make sure that an outsider (for example a competitor) is unable to read your communications?
- How can you be sure a secure electronic document sent from person A to person B and then from person B to you is the same document A sent in the first place?

It is clear that for international electronic trade to flourish, a reliable form of electronic signatures is critical. Electronic signatures, and the management processes to which they are subject, have the capability of providing the means for this to happen and of creating trust and confidence for business partners.

One of the most widespread ways to provide secure communication is to assign two uniquely and intimately bound pieces of information, which allow two or more parties to exchange information. These pieces of information are called keys:

- the *private key*, which has to be safeguarded;
- the *public key*, which can be freely distributed.

This is called public key technology. It can also be used to provide confidentiality between two parties, the sender being able to encrypt a message so that only the intended recipient can decrypt it.

Private keys are usually held on some form of storage device – today, a smart card (similar to a credit card, but with a micro-chip providing limited memory and processing capability) is very common, although there are numerous alternatives. Smart cards generally require a PIN code, or sometimes a pass-phrase, to activate them. Hence, just as with a credit card, debit card or house key, it is important to ensure neither they nor their codes fall into the wrong hands.

When an individual wants to sign an electronic document he uses his private key to perform a special function on the document (typically a text-based document, but it could be any form of electronic file – an image, an audio sample, or other types of content). The function could be merely to confirm the data on the message and about the message for future recipients or it could be to encode the document.

In addition to security issues, Electronic Signatures can be used to:

- confirm the identity of the other party - **authentication**;
- determine the authority or signing capacity of the other party - **authority**;
- ensure that the contents of any document have not been changed in any way - **integrity**;
- verify that the document has come from the claimed party - **authenticity**;
- sign a document in a legally-binding fashion - **legal commitment**;

- ensure that the original signing party cannot later claim not to have signed - **non-repudiation**.

Of course, it might be possible for anyone to acquire a pair of keys in the name of someone else, possibly an imaginary person. How would anyone else know? The solution is to put in place a process that requires the key holder to satisfy a number of conditions to prove their identity. These checks are performed by or on behalf of a trusted third party who, given satisfactory evidence, is prepared to certify that the details of the key holder are as they are claimed to be. Consequently the public key is signed by this certification authority, and is therefore known as a public key certificate. Anyone who wishes to can verify the certificate with the original certification authority who should maintain a directory of keys they have certified and a list of revoked certificates. In this way, a relying party can always be sure of the current legitimacy of the signer's public key.

An EC Framework Directive for electronic signatures came into force on 19 January 2000 (EU Member States must implement its provisions by 19 July 2001). In essence, it says that electronic signatures cannot be denied legal effects just because they are in electronic format. The directive also allows Certification Service Providers to provide their services without prior authorisation by national bodies. Member States may themselves decide how they ensure the supervision of compliance with the provisions of the directive. The directive does not preclude the establishment of private-sector-based supervision systems or oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme. However, Member States are obliged to notify the EC of any approved provision of certification services.

This directive is an important contribution to enabling secure electronic commerce within the European Union. Electronic signatures will be used increasingly in the public sector within national and EU administrations and in communications between those administrations and with citizens and businesses, for example in the public procurement, taxation, social security, health and justice systems.



## 7. Payment Systems

Traditional debt transfer systems are credit cards and bank transfer. And in B2C e-commerce, credit cards have become the prevalent form of on-line payment. This is probably due to circumstances in the US, where e-commerce first took off. There, credit cards are commonplace, but there exists no widespread system of direct bank transfer. Moreover, Americans still settle many payments with paper cheques – a means clearly not suited to electronic transactions.

However, owing to consumer security concerns about the digital transfer of credit card details across the Internet, companies with an interest in promoting electronic transactions have developed various secure payment systems involving different strengths of encryption.

Addressing consumer fears over submitting credit card details on-line, several companies have developed systems that allow more secure transactions to take place. These systems range from the use of encryption to protect credit card details to the development of new methods of payment such as electronic cash systems which involve the exchange of digital payment tokens directly between the parties.

To create trust and confidence, the payment system should be chosen carefully and an encryption system and details about data security during data transfer should be provided. However, vendors should be developing such systems as much for their own security as their customers. In cases of misuse of sensitive data, especially credit card numbers and bank details, the burden of proof is with the supplier.

<b>Comment</b>
----------------

Although it is consumers who are most concerned about giving credit card information on line (curiously, people who will gladly hand over their credit card to anyone looking like a waiter in a restaurant, will be very reluctant to provide credit card information over a highly secure system on the Internet), it is retailers who are at the greatest risk. Credit card companies are quick to do a *chargeback* (i.e. demand the payment back from the retailer) whenever a consumer has a complaint about an on-line sale. Unfortunately, a number of dishonest individuals have taken advantage of this policy, making substantial purchases and then doing a chargeback. Be sure to discuss this issue with your bank when establishing a merchant account to accept credit card payment over the Internet. Also ensure that your payment system is secure – not only the software, but staff collecting payment, printed documents with credit card data, etc.

The digital transmission of products and services has prompted calls for the development of payment technology that will allow consumers to transfer value digitally in order to pay for these products and services.

Rapid developments in on-line commerce mean that payment systems are needed not only for the sale of products and services, but also for new methods of advertising and information retrieval. Both the digital transfer of products for value and new advertising methods, such as paying consumers to view web sites or fill out questionnaires, have prompted the creation of systems which can immediately transfer value and are suitable for low value transactions. New and specially developed payment systems include smart cards (Visacash, Proton, Mondex), e-cash, cybercash (software stored on the computer), micropayment systems and loyalty schemes.

The advantages of digital cash are peer-to-peer transfers, anonymous purchasing, certainty of payment for the retailer, and suitability for low value purchases.

The Electronic Money Directives provide that electronic money institutions (i.e. undertakings other than banks and credit institutions) can issue electronic money throughout the European Union based on a single licence obtained in one Member State. These institutions also fall under a single supervisory regime.

In the different Member States, issuers may find themselves subject to differing regulations. While the issuance of electronic money is still restricted to credit institutions in some countries, in others commercial organisations are free to provide this service. The differences arise from the Member States' divergent interpretations of the activities of electronic money issuers.

## 8. Consumer Protection

### **General Information**

Legal provisions for consumer protection vary significantly between EU Member States (for example, in Germany it is not legal to offer a life-time guarantee; on advertising targeted at children the Finnish approach is very different from the British approach). Existing and prospective EU rules (enshrined in, for example, the Distance Selling Directive, the E-commerce Directive and the Data Protection Directive) aim to protect the consumer, although some of these have a corresponding downside for business. A clear, common set of consumer protection standards still does not exist in Europe.

### **Commercial Communications**

Analysing how off-line and on-line promotion influence entertainment consumption, Forrester found that web sites and e-mails are as effective as off-line promotion via magazine ads, billboards, and theatre previews. Tips gathered in chat rooms and instant messages are the most effective means of on-line promotion. Comparing individual off line promotional tools with on-line ones revealed that Web promotion can surpass the power of television.

Commercial communications are essential for the financing of electronic business and for developing a wide variety of new, charge-free services. In the interest of consumer protection and fair-trading, commercial communication, including discounts, promotional offers, and promotional competitions or games, must meet a number of transparency requirements.

Both the commercial nature of the communication and the person for whom the communication is provided should be clearly identified. In the case of commercial communications via

e-mail, the commercial nature of the message should be obvious as soon as the consumer or professional receives the message. Moreover, the advertiser must honour opt-out lists, ie, public lists of people who have explicitly asked not to receive unsolicited commercial e-mail.

The Electronic Commerce Directive enables Member States to both authorise and prohibit the sending of unsolicited commercial communications by electronic mail.

Where Member States allow it, it must be "clear and unambiguously" identifiable as such as soon as it is received.

Besides, Member States can choose between:

- an opt-in system (prior consent of the recipient required before the sending of unsolicited commercial communications); or
- an opt-out system (no sending of unsolicited advertising to individuals who have mentioned in a register that they do not wish to receive it). These opt-out registers would have to be checked regularly by providers of unsolicited commercial communications.

**Suggestion**

Be careful with unsolicited commercial e-mail, often known as SPAM. Although the E-commerce Directive has taken a lenient view on SPAM, most Internet service providers (ISPs) do not. Indeed, most ISPs have an acceptable use policy (AUP) which expressly forbids SPAM and which you must agree to when subscribing to the ISPs services.

At the least, most ISPs will close your account with little or no warning if you break the AUP. Some will also charge you costs (the bulk of the costs of transmitting SPAM are carried by the ISPs who have to pass it on to their customers if they cannot collect it from the persons responsible for the SPAM). Having your e-commerce site, or even just your e-mail, suddenly taken down can obviously cause serious problems to your business.

Moreover, most Internet users do not like SPAM. The result being that SPAM can actually have a negative effect, costing you customers rather than bringing you new customers.

Nevertheless, e-mail marketing can be effective. However, you should use opt-in lists – that is lists of people who have indicated an interest in receiving targeted e-mail offers. There are a number of highly reputable companies offering not only opt-in lists tailored to your target customers, but a variety of services that allow you to monitor results, do test runs and change tactics mid-mailing. To ensure you are dealing with a reputable e-mail marketing company, ask for names of clients and check with those clients.

## 9. Data Protection

Corporate marketing departments have always been hungry for customer data and the Internet has made it easier than ever before to collect that data. But there are some rules that must be respected in the collection and use of data about customers and visitors to your web site. Special attention needs to be paid to national data protection regulations and especially to the EU Data Protection Directive 95/46/EC of 24 October 1995 and to the Telecommunications Data Protection Directive 97/66/EC of 15 December 1997. Complying with data protection law is a complex process that requires a comprehensive and consistent management approach throughout the whole organisation.

The Data Protection Directive aims to ensure the free flow of data within the Union while safeguarding the fundamental rights and freedoms of individuals. It guarantees the confidentiality of electronic messages and prohibits any kind of interception or surveillance of such electronic messages by any party other than the senders and intended recipients.

According to the directive, Member States must determine the conditions under which the processing of personal data is lawful. In any event the directive provides that personal data can only be collected for "specified, explicit and legitimate purposes" and must be processed in a way which is compatible with these purposes.

When collecting data about an individual, there are several considerations that must be followed.

### **Collecting**

Personal data can only be collected and processed by the provider if permitted by some law or if the individual has unambiguously given his consent.

### **Use**

Data must not be processed for any purposes incompatible with those for which the data was initially collected. Data cannot be transferred to third parties without agreement from the data subject. Security measures must be taken to protect the personal data against any accidental or unlawful destruction or accidental loss. Data should not be kept longer than necessary for the purpose for which it was collected.

### **Access**

Data should be accurate, complete and kept up-to-date. The customer must have access to any personal data concerning him/her that is being processed or kept. A request for correction or deletion of incorrect personal data must be granted within a reasonable period of time. The customer must have the possibility to opt-out of the processing operation of his/her data and to refuse certain use of the data.

The level of security must be appropriate to the risk presented by processing and the nature of the data. The individual has the right to object to the processing of personal data relating to him if it is used for the purpose of direct marketing. Also concerning payment systems are the compliance with data protection principles (specified and lawful purposes, adequate, relevant and not excessive, accurate, securely held, not transferred to third countries without adequate protection, consent).

It should be noted that detecting interception or surveillance is very difficult. However, there are numerous security systems on the market to prevent against surveillance.

## **Safe Harbour**

The Data Protection Directive prevents transfers of consumers' personal data to third countries where the level of data protection is considered "inadequate". The Data Protection Directive addresses every individual's right to privacy with respect to the processing of personal data, whether processed, stored or used in any fashion. Information can only be used for the purposes for which it is obtained, be kept as long as necessary, and must be kept up-to-date.

Because US data protection is non-statutory and there is no government data protection office, it is regarded as inadequate by definition. Yet blocking the transfer of business data to the USA is widely regarded to be all but unthinkable. Therefore, the European Commission adopted on 26 July 2000, a decision on the adequacy of the level of data protection in the US with the EU Data Protection Directive. The decision entered into force on 1 November 2000. Any transfer made before this date is not subject to the decision.

The Commission decision specifies the conditions under which there is an adequate level of protection in the US for the transfer of data from the European Community to the United States. By agreeing to the safe harbour principles, US business will therefore be able to collect data and transfer personal data between the US and EU Member States. This way US organisations can keep in line with the European data protection principles, create trust and confidence and develop best business practice.

To guarantee a smooth flow of data from Europe to the US it is important to follow this issue. The Safe Harbour is intended only for the US. There are (for example, with Hungary and Switzerland), and will be, other agreements with other countries.



## 10. Intellectual Property

Intellectual property rights (IPR) consider creative work as a form of property and give the owners of the creative work the right to use, rent or sell some or all of their rights over that property. Usually, IPR gives the creator an exclusive right over the use of his/her creation for a certain period of time.

Intellectual property rights can be divided into several categories:

### **Copyright and rights related to copyright**

Copyright is a form of property right attached to an original work and which controls the right to copy the work for a period lasting up to 70 years after the death of the author, depending on the type of property being protected. A "Work" can be a literary or artistic work including books and other writings, musical compositions, photographs, advertisements, maps, catalogues, web page paintings, sculpture, computer programs, films and certain databases. Copyright encourages and rewards creative work as it makes it unlawful to copy the results of someone else's efforts without their permission.

Related (also called "neighbouring") rights are granted to certain well-defined categories of persons who are involved in the business of musical or audio-visual creation, such as performers (e.g. actors, singers and musicians), producers of phonograms (sound recordings), and producers of first fixation of films, and broadcasting organisations. The duration of related rights is fifty years following the date of the performance, the fixation, or after the first transmission (for broadcasters). Throughout Europe, copyright protection does not require formal acts such as registration or copyright note.

**Case Study**

E-Marketing Clinic is a small one-woman operation offering consultancy services to small and medium sized companies wanting to market on the Internet. The company has a comprehensive web site with downloadable reports and guides to help people understand and implement e-marketing. This information is an effective tool for establishing the credibility of E-Marketing Clinic. Indeed, the company has been quite successful and Lisa, the owner, has established a name for herself in Internet marketing circles.

One day, while using a search engine to look for new information in her field, Lisa discovered a link to a web site that appeared to be very similar to hers. She visited the site and was surprised to discover that someone had taken all her material, claimed it as his own and posted it on his web site.

Lisa contacted her lawyer, who promptly issued a "cease and desist" order to the plagiarist and his ISP, and the copied web site disappeared right away. Surprisingly, this has happened to Lisa several times since and she now makes it a regular habit to monitor search engines for illegal copies of her web site and documents. She also publishes a copyright notice on every page of her web site. Strictly speaking, this isn't necessary. But it probably acts as a deterrent to the casual plagiarist.

International Regulatory Framework and EU Regulatory Framework coexist in the field of copyright. The key international agreement is the Berne Convention for the protection of literary and artistic works that has been ratified by more than 120 countries.

The European Regulatory Framework provides Directives on:

- the legal protection of computer programs

- the legal protection of databases
- rental and lending rights and on certain related rights
- cable and satellite broadcasting
- term of protection

The European Commission Proposal for a Directive of 10 December 1997, on the harmonisation of certain aspects of copyright and of related rights in the Information Society deals both with legal and technical aspects. The directive covers reproduction rights, communication to the public rights, distribution rights, and legal protection of anti-copying and rights management systems. The proposal requires that Member States continue to provide network operators with an exception from the reproduction right for certain technical acts of reproduction (such "cache" copies which are stored on Internet servers as users browse the World Wide Web) and recognise that Member States may provide rights-holders with fair compensation for private copying by analogue as well as digital means, in accordance with their legal traditions and practices.

The directive aims to adapt the existing IPR European framework to the on-line environment and to comply with international commitments. It will stimulate creativity and innovation by ensuring that music, films and all materials protected by copyright enjoy adequate protection throughout the single market. It will facilitate cross-border trade in copyright-protected goods and services, with particular emphasis on new electronic products and services (both on-line and on physical carriers such as CDs). In the case of private copying, photocopying and illustrations for teaching and scientific research, the proposal specifies that right holders must have access to fair compensation.

## **Protection of Databases**

### **Copyright Protection**

The objective of the directive on the legal protection of databases is to afford an appropriate and uniform level of legal protection of databases in any form, as a means to secure the remuneration of the maker of the database. It protects via copyright a database which “*by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation*”. It does not protect the contents of the database, which may or may not be protected by copyright or related rights, but the database itself.

The directive excludes the protection of computer programs used in the making or operation of databases accessible by electronic means but covers:

- the legal protection of computer programs
- rental right, lending right and certain rights related to copyright in the field of intellectual property
- the term of protection of copyright and certain related rights

The protection expires 70 years after the death of the author.

### **The New Economic Right**

The new economic right protects substantial investment made in obtaining, verifying or presenting the contents of the database. It lasts for 25 years from 1 January of the year following the completion of the database.

### **Industrial Property**

Industrial property provides a monopoly right of the exploitation of certain intellectual creations:

**Trademarks**

Trademarks provide protection for signs, which distinguish the goods or services of one undertaking from those of other undertakings. In most countries registration is necessary. There is no time limit for the protection offered, provided the appropriate formalities for renewal of the registration are complied with.

**Patents**

Patents are protected primarily to stimulate innovation and creation of technology. The social purpose is to provide protection for the results of investment in the development of new technology, thus giving innovators the incentive and means to finance research and development. The protection is usually given for a certain term, typically 20 years. It should be noted that United States patents are not recognised in the European Union. Also, at the time of writing, business models can be patented in the US, but not in the EU.

**Industrial designs**

Industrial designs provide protection for the shape or appearance of a design that is industrially exploited. Registration protects industrial design for a limited time, generally 10 to 15 years.

**Unfair competition**

Competition law can provide protection against a number of commercial practices that involve the unlawful acquisition of a company's intellectual portfolio, such as "know how" or trade secrets. Both EU and national competition law apply and rules may differ from one country to another. There is no particular body of competition law that applies to the Internet, so a new perspective is given to established issues.

**Domain Names**

New and specific trademark-related e-commerce problems regarding Internet domain names are beginning to occur and will doubtless star in upcoming legal cases. Questions arise over the international domains, particularly .com. What happens if a company in one country acquires the .com for its name (newcompany.com for instance) and a year later another company from another country with a trademark for the same name claims and wants to register it? What happens if two companies, from different countries and both holding trademarks within their countries, have a dispute over who holds the right to a particular name? These issues have not yet been clarified, but doubtless will be raised and clarified in the courts in upcoming years, particularly as new international top level domains, such as .eu, are established.

What is clear, following several landmark legal cases, is that domain name squatting is illegal. Domain name squatting is the act of acquiring a domain name that obviously belongs to someone else, either because the other party has a trademark on the name or has clear ownership of the name (ie. a celebrity or politician), with intent to sell or lease the domain name to the rightful owner.

**The .eu domain**

The growing scarcity of international top level domains makes it more and more difficult to find a short and attractive domain name. The .eu domain is an initiative by the European Commission to create a new top-level domain for European business.

## 11. Taxation and E-commerce

### **Direct Tax**

It is unlikely that e-commerce will have any significant impact on direct taxation (e.g. income tax, corporation tax and taxes on profit) in practice.

The fundamental beauty of the Internet, from the perspective of those who wish to minimise their tax administration, is the ability to perform transactions at a distance. Selling electronically is an obvious opportunity for a business to either reduce or avoid a tax footprint outside the country where it is resident. A business will still be liable to tax where it is resident, but it does not necessarily have to have a taxable presence elsewhere to meet its commercial objectives.

Web sites and servers through which sales are made cannot constitute a taxable presence in another country. A web site alone is not a fixed place of business and so does not create a taxable presence in another jurisdiction. Only if the business to which the web site belongs also owns or rents the server, and if the activity carried out via the web site is not within the normal exclusion for preparatory or auxiliary activities, will a taxable presence exist. In this instance, using an ISP to host a site allows a company to avoid having a taxable presence in any other country.

### **Indirect Tax**

There are however important considerations for indirect taxation (e.g. Value Added Tax or sales tax) such as when different rates of tax apply to goods and to services. A book (a product) may attract one rate of tax, but in digital form be considered a service by the tax authorities and thus attract a different rate of tax. It should be noted that the EU recognises digitally delivered

products such as software, digital music, digital books, etc as services.

## VAT

The Internet enables companies to reach customers without regard for national boundaries. That said, cross-border sales must nevertheless comply with specific indirect taxation rules like Value Added Tax (VAT) and withholding taxes. Payment of VAT is determined based on what, where and to whom goods and services are sold. The rules within the European Internal Market differ for goods and services.

### Goods

<b>VAT and Goods</b>	
<b>Customer</b>	<b>VAT Requirements</b>
Same EU Country	You charge local VAT rate
Business in different EU country	Customer submits and pays VAT in her country
Consumer in different EU Country	If under threshold, customer pays VAT at your rate and you submit VAT; if over threshold, customer pays VAT at own rate and you submit in customer's country
Non-EU country	VAT is zero-rated

The VAT liability on supply of goods is determined by the physical movement of goods when a sale takes place and by the status of the customer. The way goods are taxed in respect of VAT is not affected by the growth of the Internet. The existing VAT system applies to goods purchased electronically and then delivered by traditional means.

Where a business established in the EU sells goods to a private citizen (i.e. not engaged in business) within the EU, the VAT rules for mail order apply. These are based on thresholds. Each EU country has a threshold of either 35,000 or 100,000 Euro per year. If a company's sales of goods to consumers in another Member State exceed that threshold, the company must hire a tax representative in that Member State, register for VAT in that Member State, charge customers VAT at that Member State's rate and have their VAT representative file VAT returns in that Member State. If sales are below the Member State's threshold, VAT is charged at the rate applicable in the company's country and is filed locally. There is currently a lack of harmonisation in VAT rates, with standard rates ranging from 15-25% in the EU.

Some individuals and organisations are considered "non taxable persons". They include private individuals, public bodies, charities and some businesses with low turnover or wholly exempt activities.

## Services

### VAT and Services

Customer	VAT Requirements
Same EU Country	You charge local VAT rate
Business in different EU country	Customer submits and pays VAT in her country
Consumer in different EU Country	Customer submits VAT at your rate, you submit locally

Non-EU country	No VAT
----------------	--------

The Internet is not only an efficient order management medium, but also a means of delivering a product itself. Customers can conveniently download any form of software such as digitised music or games, or other intellectual property such as training material or consultants' advice. Such products are, from the perspective of EU VAT legislation, classified as supplies of services and so taxed as services. Moreover the EU mail order rules regarding turnover thresholds do not apply.

The current VAT rules for services do not adequately address the supply of services delivered on-line by digital means, notably in the case of services traded between EU and non-EU countries. At the time of writing, electronically delivered services originating within the EU are always subject to VAT irrespective of the place of consumption, whilst those from outside the EU are not subject to VAT even when delivered within the EU. This situation has the potential to constitute a major distortion of competition and to place EU service providers at a disadvantage in relation to non-EU service providers. However, this could soon change.

The European Commission has presented a proposal for a directive to modify the rules for applying VAT to certain services supplied by electronic means as well as subscription-based and pay-per-view radio and television broadcasting. The objective of the proposal is to create a fair market for the taxation of digital e-commerce in accordance with the principles agreed at the 1998 OECD Ministerial Conference. A basic principle of the EU VAT system is that no new or additional taxes are needed for e-commerce. Existing taxes should be adapted so that they can apply to e-commerce.

The proposal mainly concerns the supply, over electronic networks (i.e. digital delivery via the Internet), of software and computer services generally, as well as information and cultural,

artistic, sporting, scientific, educational, entertainment or similar services.

The proposal will ensure that when these services are supplied for consumption within the European Union, they are subject to EU VAT, and that when these services are supplied for consumption outside the EU, they are exempt from VAT. The proposal also contains a number of facilitation and simplification measures aimed at easing the compliance burden on business.

Non-EU operators would only have to register for VAT purposes where they undertake business-to-consumer transactions (a different regime applies to business-to-business). Where their annual sales to consumers in the EU exceed a minimum turnover threshold of 100,000 Euro, non-EU operators would be required to register for VAT purposes, but only in a single Member State (they could choose any Member State where they supplied services). They would then charge VAT at the rate applicable in the Member State they have chosen and only have to deal with a single tax administration within the EU.

## **Withholding Tax**

Many countries have withholding taxes on certain types of income originating within their borders. These are withheld at source by the payer and are usually based on gross revenues. For a business they are at best a cash flow cost but at worst a real cost if full credit for withheld taxes cannot be obtained against the business's home country tax liabilities. The types of income to which withholding taxes are most typically applied are dividends, interest, and, more significantly for a company doing business electronically, royalties. Some countries, most notably those in the developing world, also have withholding taxes on service or technical fees paid abroad. However, no country has yet introduced a withholding tax specifically on income generated by electronic means, so a company will not, in

principle, increase its exposure to withholding taxes by doing business on the Internet.

## 12. Liability of Intermediaries

To remove existing legal uncertainties and to avoid divergent approaches between Member States, the E-commerce Directive establishes an exemption from liability for intermediaries where they just transmit information between third parties. Service providers have only limited liability for other "intermediary" activities such as the storage of information (hosting) or enhancing onward transmission (caching). This implies that in most circumstances, as long as ISPs do not take an active involvement in the information they are transmitting and are not aware they are transmitting illegal content, they are not liable for transmitting it. If an ISP learns that, for example, a web site it hosts includes illegal material, the ISP is normally required to remove this material as soon as possible.

### 13. And the Future...

E-commerce and its underlying technologies are developing so quickly, it is a dangerous game to guess where they are going. Nevertheless, some clear trends are apparent.

Mobile e-commerce is a key growth area, which Europe is just experimenting with at the time of writing. Already it is possible to browse the web and buy things with a mobile telephone. How this will pan out and what the killer applications will be are not clear now. But business and investors are excited about the possibilities, and new mobile e-commerce ventures are popping up every day. More importantly, there are more mobile telephones than PC computers in Europe. So, there can be little doubt that in five years time, a European browsing the net is more likely to be doing so via a mobile device than a computer. Indeed, this is already the case in Japan. Clearly, when the consumer is mobile in a Europe without frontiers, there will be some complex regulatory issues in the areas of applicable law, jurisdiction and VAT that will need resolving.

Ubiquitous Internet and computing is another growth area. This involves devices other than a PC computer connected to the Internet. These devices could be anything from the climate control system of a house which can be controlled from the owner's mobile telephone, to a rubbish bin that notices when certain food containers are thrown away and reorders from the local supermarket. More elaborately, intelligent agents in a house's central computer might negotiate with various electrical generation and supply sources to obtain the best electricity deal for the owner. When household agents negotiate with intelligent agents belonging to an electrical company (or telecommunications company or any other service), there are some interesting liability and contractual questions that will need to be resolved.

At the same time, many other exciting avenues of e-business are being explored and likely some commonplace technologies of tomorrow have yet to be envisioned today.

In any event, the European Commission is preparing a legal framework for electronic commerce that will ensure consistent laws across the EU, thereby facilitating trade. This should largely be in place in the next few years. Then it will only be a matter of ensuring that legislation keeps up with the technological developments – or at least doesn't fall too far behind.

### **Concluding Words**

This guide reflects the current status of European legislation and is based on the experience of available best practice. However, legislation and business models are rapidly changing in the world of e-business. Up-to-date legal resources should be consulted for new information, and legal advisors consulted for detailed information and interpretation.

The Commission provides a lot of information on the Internet and, as an umbrella information source, we recommend the e-commerce web site: <http://www.eRevolution.lu>. Here you can find most of the relevant issues, with operable links to the other services of the Commission relevant to e-commerce.

The authors welcome feedback on this publication to improve it in future editions and to serve the needs of our customers as best we can.