

ANALYSIS AND DEFINITION OF COMMON CHARACTERISTICS OF TRUSTMARKS AND WEB SEALS IN THE EUROPEAN UNION

FINAL REPORT

Authors:	Dr. Ronald de Bruin (ECP.NL), Ewout Keuleers (CRID), Christophe Lazaro (CRID), Prof. Yves Pouillet (CRID) and Marjolein Viersma (ECP.NL)
Version:	2.3
Date:	February 2005
Contract no:	B5-1000/03/000381

Foreword

In our opinion, trust and confidence is pivotal to the long-term development of e-commerce. Without trust, e-commerce cannot fully bloom. A trustmark can add value to the establishment of trusted relationships between businesses and consumers. At the same time, we do realise that trust and confidence in a trustmark is just as important. Through this research we hope to have provided more insight in the underlying multi-disciplinary factors that play a role in this. As such, this research has delivered insight in the business and consumer acceptance of trustmarks, the extent to which trustmark schemes meet legal requirements and the commercial viability of trustmark schemes.

There are several people we would like to acknowledge for their contributions. First, we would like to thank BEUC, UEAPME and UNICE for their assistance in approaching their national member organisations to contribute to the consumer and business surveys. We would like to thank the national organisations that have responded to the surveys. Together, they provided valuable input for the research. Also, we are grateful to the trustmark schemes that responded to the telephone interview and their willingness to provide any information on their commercial operations.

ECP.NL, platform for eNetherlands / Centre de Recherches Informatiques et Droit (CRID)
Leidschendam (NL) / Namur (B), 22 January 2005

Executive summary

Introduction

In 2000, the European Commission launched an initiative to strengthen consumer confidence in e-commerce. This work focussed on the role and effectiveness of trustmarks in the European e-commerce market place.

Following a joint project by stakeholders, a draft set of European trustmark requirements was produced by the Federation of European Union Employers' Federations (UNICE) and the Bureau Européen de Consommateurs (BEUC). These requirements aim at setting a high (but voluntary) standard for e-commerce trustmarks and include proposals for certification of the trustmarks and monitoring of their compliance with the requirements.

At the same time, evidence in the market place suggests that trustmarks have difficulties both in achieving brand recognition by consumers and in becoming commercially viable and sustainable operations. Therefore, it would be useful to have more in-depth information about the role and potential of trustmark schemes in the e-commerce marketplace in the European Union.

On 22 December 2003 the ECP.NL/CRID consortium were awarded a contract by the European Commission (DG SANCO) to analyse and define the common characteristics of trustmarks and webseals in the European Union.

Research approach

The purpose of this research was to obtain an analysis of the e-commerce market from the perspective of trustmark schemes. This analysis should allow drawing conclusions:

- § as to the usefulness of trustmarks for consumers, regarding the extent to which such trustmarks contribute to strengthening consumer confidence;
- § about the extent to which trustmarks are commercially viable operations, or can be made viable;
- § as to the conditions under which trustmarks would gain most acceptance from consumers and businesses alike. This would mean in particular issues related to independence, monitoring and enforcement, but also the administration and management of such operations, and their costs;
- § on the extent to which trustmarks benefit different types of e-merchants (major enterprises as opposed to SMEs), and to which extent they substitute (or have potential to substitute) brand recognition on the e-commerce market.

The research methodology defined four distinct phases. First, a number of European trustmark schemes were identified, after which a limited number of trustmark schemes were selected. The next phase concerned a study of factors relevant to the success of trustmark schemes i.e., critical success factors. In the last phase, conclusions were drawn and recommendations were made. In the end, the research has delivered a business and consumer analysis (including a brand value analysis), a legal analysis on trustmark schemes and a commercial viability analysis on trustmark schemes.

For the purpose of the analysis, the following trustmark schemes have been identified and selected: BBB*OnLine* (commercial viability analysis only), Confianza Online, Euro-label, Luxembourg e-commerce certified, Thuiswinkel, Trusted shops, TrustUK, Web Trader, WebTrust and QWeb.

Business and consumer analysis

The business and consumer analysis zoomed in on the aspects of business and consumer acceptance, brand value and consumer experience. The analysis was performed through an online survey conducted with national business and consumer representatives. In total, there were eighteen valid responses from consumer organisations and seventeen from business organisations.

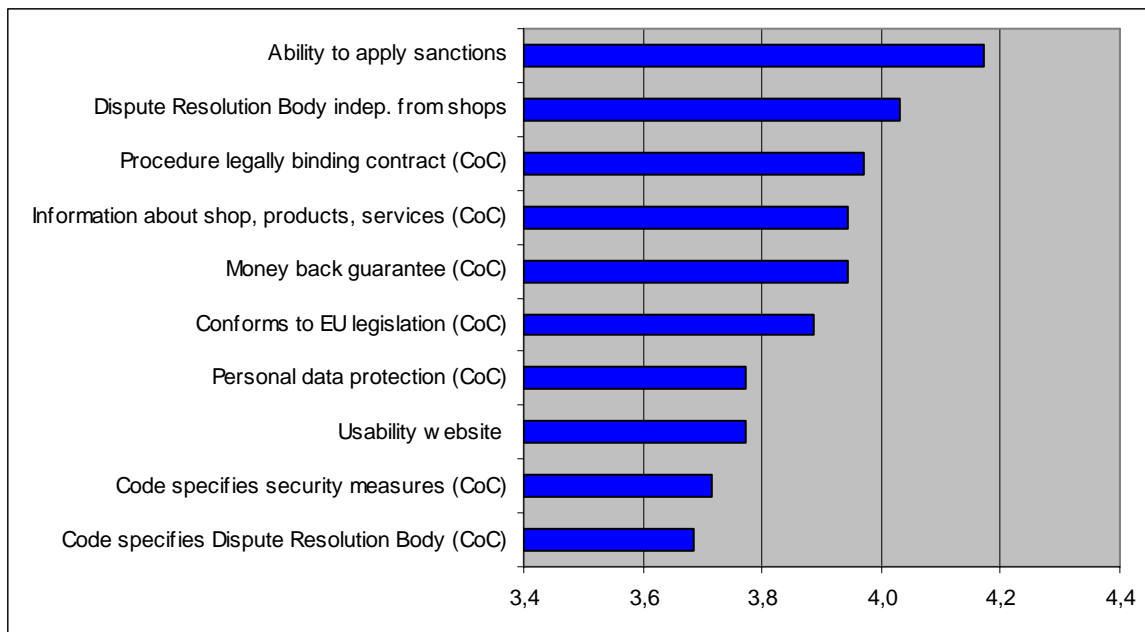
When evaluating the response to the online questionnaire the following conclusions can be drawn about the general opinion of the target groups:

1. Consumer representatives in general value the critical success factors much higher (very important) than the business representatives (important)
2. The response of business organisations to the online questionnaire (21%) is much lower than the response of consumer organisations (46%)
3. Based on the telephone conversations with European business organisations the level of knowledge of and enthusiasm about trustmark schemes for online shops seems low.

This indicates that consumer organisations feel the need for self-regulation in e-commerce, but the awareness in business organisations is relatively low.

As a result of the business and consumer acceptance analysis, the table below presents a combined top-10 ranking of critical success factors according to the business and consumer organisations.

Table 0.1¹
Top 10 CSF – business and consumer combined



¹ Respondents have rated the critical success factors on a five point scale; 1 standing for “not important” to 5 for extremely important”.

The recommendations to increase the acceptance of a trustmark scheme are:

1. The most critical success factors are those that are contained in the code of conduct. Making sure the code complies with the applicable (EU) regulations is very important. This could be achieved by drawing up a model code of conduct at European level. Individual trustmark schemes can use it to save on legal expenses and uniformity of the codes might increase consumer confidence in trustmarks in general.
2. A “money-back guarantee” is supported by both consumer and business representatives. However, this guarantee is usually not given in a trustmark code of conduct. It might be wise for a trustmark scheme to include this benefit.
3. It is very important that a trustmark scheme has the power to take appropriate action when a certified shop does not comply with the code of conduct. It is advisable for a trustmark scheme to have more than one possible sanction (withdrawal of the logo).
4. The independence of the dispute resolution body should be ensured.
5. Trustmark schemes should be transparent. The acceptance of a trustmark scheme by potential clients (online shops) and consumers cannot be increased when they do not know what the benefits are.

With regard to brand value:

1. It is important for the success of a trustmark that it has a strong brand. When an organisation which already has a strong brand starts a trustmark scheme this is easier to achieve than starting a new brand.
2. A small minority of the responding business representatives think that joining a trustmark scheme adds substantial value to the brand of an online shop. So it is advisable for a trustmark scheme to research its influence on consumer confidence and show the results.

In the field of consumer experience the following recommendations can be made:

1. Consumers who take the effort to visit a trustmark’s website should be able to find the information they look for easily. Investing in the usability of such a website is important.
2. According to the respondents, most consumers prefer to communicate in their own language. The best alternative is English, but using this language would decrease consumer confidence.
3. It may be effective to use a combination of informal, global information and formal, detailed information on the website of a trustmark scheme.
4. The respondents think the website of a trustmark should contain a list of certified online shops. It must be possible to verify certification by clicking on the logo of the trustmark on a certified website.

Legal analysis of trustmark schemes

The legal analysis concerns a benchmark on trustmark schemes based on legal criteria that stem from sources of hard law and soft law. From these different normative sources, the highest common criteria were identified. This comparative process resulted in a list of more than 40 general selection criteria. Afterwards, this general list was converted into a more functional synopsis. In function of the phases of the *life cycle* of a trustmark scheme, i.e., from conception, dissemination to enforcement, different criteria were grouped and ordered in a more pragmatic and systematic manner.

For the purpose of the legal assessment, the following phases in the trustmark scheme’s life cycle were identified: Elaboration of the trustmark scheme, Information on the trustmark scheme, Participation in the trustmark scheme, Code of conduct, Proactive monitoring, Complaints procedure, Enforcement and Relations with protagonists.

Eventually, this “pragmatic list” of criteria was used to identify 14 legal criteria a trustmark scheme should necessarily have. These so-called *must-have* criteria have been chosen due to their legal added value; the extent to which they add any value to already existing hard (positive) law. In contrast to the remaining *nice-to-have* criteria, the list of 14 must-have criteria allows a better understanding of the legal quality of a trustmark scheme and their respective positions in relation to the other schemes. These must-have criteria are:

1. Legitimacy of the scheme
2. Access and clearness of the code of conduct
3. Information on trustmark scheme’s functioning
4. Assessment
5. Feedback
6. Applicable law and competent jurisdiction
7. Confirmation process
8. E-platform security
9. Customer service
10. Protection of children
11. Proactive monitoring
12. Complaints procedure for solving disputes
13. Enforcement system
14. Relationship with consumers

The evaluation was performed through desk research, while making use of information that is publicly made available on the trustmark schemes’ website. In case trustmark schemes are part of a hierarchical structure, the trustmark scheme at the lowest level of the hierarchy was assessed. This allowed a more meaningful comparison between trustmark schemes. At the same time, the lower level has the highest impact on subscribers and consumers. Because trustmark schemes may change their information over time, it should be noted that the evaluation is made at a certain time. Hence, the results of the evaluation are time-stamped. Finally, it is fair to say that despite the objectiveness of the criteria themselves, it cannot be excluded that this benchmarking activity to a certain extent had a subjective character.

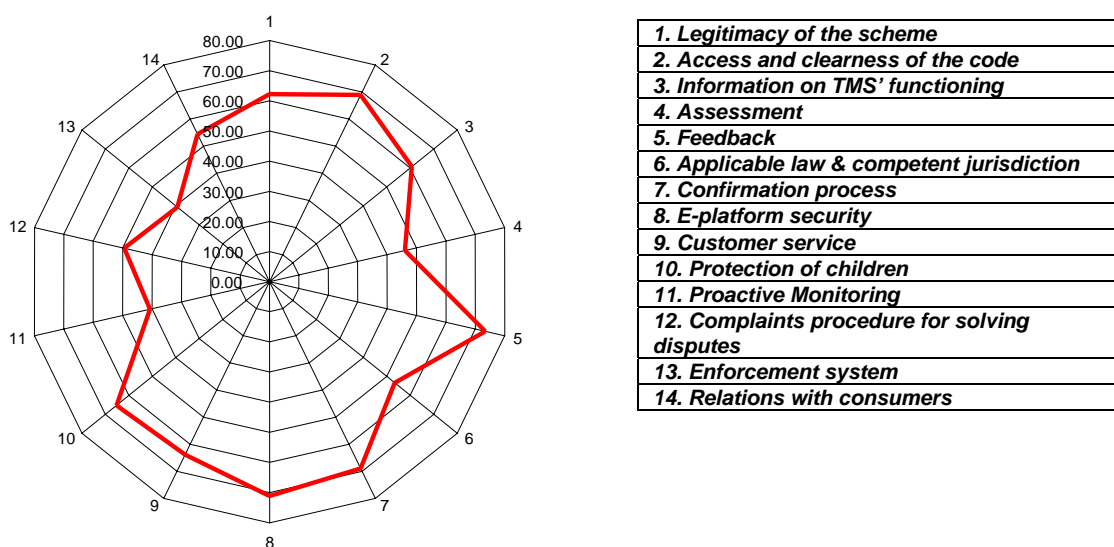
As a general finding, the evaluation demonstrated that there are as many differences in meeting the criteria as there are trustmark schemes. It seems that there is (almost) no (positive) correlation between criteria. Although on a micro level a positive evaluation for, e.g., legitimacy, may indicate transparency on the management structure of the scheme, this is not so on a macro level of the life cycle’s phases or must-have criteria. Vice versa, the fact that a particular criterion is evaluated in a negative manner does not by definition imply that this is also the case for other criteria.

Indeed, based upon the present review of criteria, one has to conclude that some trustmark schemes have very good evaluation values for one, two or more phases (of the life cycle) or must-have criteria. However, of the 9 trustmark schemes, there is not one that has positive values (three or more) for every must-have criteria. In this context and from a legal point of view, it is difficult to understand why certain trustmark schemes demonstrate their quality while elaborating and implementing good self-regulatory principles, but, e.g., fail to inform consumers in a transparent way or do not allow user-friendly registration methods for codes of conduct and other rules. One explanation for this can be found in the fact that some trustmark schemes prefer to start with a small-scale model that grows to a full-scale trust model, this instead of kicking off with it.

The figure below clearly demonstrates that the evaluation of the 14 must-have criteria is not very consistent. Some criteria, e.g., elaboration of the Code of Conduct or protection of

children, are evaluated in a positive manner, while other criteria seem to have a rather low score. This trend is particularly valid for the monitoring and enforcement mechanisms. We underline that the three metacriteria, – i.e., criteria n° 11 (proactive monitoring), 12 (complaints procedure for solving disputes) and 13 (enforcement system) – have a negative average evaluation between 39% and 49%. In other words, the scheme can be as comprehensive and consumer friendly as one could wish, if its principles are not enforced, the quality and the long-term existence of the trustmark scheme can be questioned.

Figure 0.2
Overview of 14 *must-have* criteria



A second trend is that most of the trustmark schemes are characterised by a lack of 'European sensitivity'. In particular, this concerns a lack of multilingual information, lack of articulation and co-ordination between the different trustmark schemes and a lack of reference to (and involvement in) the existing EU initiatives regarding e-confidence and consumer protection. Therefore, it is recommended that trustmark schemes provide bilingual or multilingual information in order to facilitate cross-border confidence. Trustmark schemes could reconsider their geographical scope and develop mutual recognition agreements with trustmark schemes in other countries or regions. In addition, trustmark schemes could be required to provide transparent and adequate information on relevant EU initiatives. Trustmark schemes could also be connected to the European Extra-Judicial Network (EEJ-Net) for cross-border dispute resolution.

In addition, many trustmark schemes do not sufficiently meet the European trustmark requirements. At the same time, these requirements do not directly address some important aspects of trustmark services. For example, they do not sufficiently insist on complaint-handling processes and alternative dispute-resolution mechanisms.

Commercial-viability analysis

For the purpose of this analysis, the trustmark-scheme business models were assessed from an organisational and financial perspective. Three baseline organisation models were defined i.e., a stand-alone trustmark scheme, a trustmark scheme based on a hierarchy and trustmark schemes that operate in a horizontal network.

The financial model includes different cost modules and revenue streams that are specific to a trustmark scheme's start-up phase and its operational phase. In order to assess the financial sustainability of a trustmark scheme, two financial key-performance indicators were used. The first indicator is that a trustmark scheme generates at least as much revenue as it costs. The second indicator used is the moment in time where the break-even point is reached. For the purpose of analysis, a reasonable point in time is defined as less than 2 years.

The gathering of data was performed through desk research and telephone interviews with the 10 selected trustmark schemes. This allowed a comparison between the theoretical model and the business models used in practice.

The analysis demonstrated that a variety of organisation models exists amongst the selected trustmark schemes. Some have a hybrid model i.e., a combination of baseline organisation models. All trustmark schemes but Web Trader, which ceased its operations after 2 years, are still operational today. All initiatives have existed for 2 years or more.

All trustmark schemes have provided information on their profit or loss during the start-up phase, except for Thuiswinkel that did not distinguish a start-up phase. Three Trustmark schemes have indicated they made a profit during this phase, but no trustmark scheme was able or willing to provide their profit margin. Six of them operated at a loss, of which one had a loss margin of 24% and five a loss margin of 100%. Only one trustmark scheme wanted to specify when they reached a break-even point, namely between 6 and 12 months.

All trustmark schemes but Luxembourg e-commerce certified (because they are not operational yet) provided information on their profitability in the operational phase. Five indicated to be profitable, while two of them were willing to specify that their profit margin is 3% and 8%. 2 Trustmark schemes operate on a break-even basis. One of the respondents indicated to be able to operate at a break-even point, because the hosting organisation absorbs the organisational costs for the secretariat. Two Trustmark schemes are making a loss. Their loss margins are 11% and 90%. Hence, the vast majority of the selected trustmark schemes are profitable or operate on a break-even basis.

Of the seven respondents that indicated to operate on a break-even basis or even make a profit, four specified the period after which they had reached their break-even point. Two Trustmark schemes reached their break-even point within 6 months, of which at least one managed to do so during the start-up phase. One Trustmark scheme reached this point between 18 and 24 months and one needed more than 24 months. Hence, at least three trustmark schemes managed to reach their break-even point at a reasonable point in time (less than 2 years).

Figure 0.3
Profit or loss operational phase



Given the analysis above, one can argue whether trustmark schemes that obtain sponsorships are truly commercially viable or not. This actually depends on the nature of the sponsorships i.e., their source and whether they are incidental or structural. From an economic perspective, the trustmark scheme that operates on a break-even basis because the secretarial costs are absorbed by the hosting organisation is not commercially viable by itself. However, due to this structural sponsorship this trustmark scheme is able to sustain its operations. Fact is, however, that at least three and a maximum of six of the assessed trustmark schemes manage to operate with a profit or at a break-even point in the end and to reach their break-even point at a reasonable point in time. Hence, it can be concluded that at least three and a maximum of six of these trustmark schemes are commercially viable.

Organisations that provide the trustmark scheme as their only service have a negative correlation with commercial viability. Hence, the provision of a larger service portfolio next to the trustmark scheme itself is a critical success factor.

The following top-7 list of critical success factors were identified based on the information provided by the selected trustmark schemes:

1. Awareness with business and consumers;
2. Highly elaborated and robust code of conduct;
3. Effective enforcement mechanisms;
4. Number of trustmarks issued (leading to user-fee revenue);
5. Trust in (independent) organisation that operates the trustmark scheme;
6. Stakeholder support;
7. Low up-front and operational costs.

Interesting to note is that some of the respondents stated that if they could start all over again, they would have focussed more on creating awareness with website owners, rather than consumers, because the demand comes from them.

With regard to enforcement, one respondent remarked that they would have started earlier with adding stronger compliance and enforcement mechanisms to the trustmark scheme. However, if this had been done too early, the stakeholders would not have accepted the scheme. Because of its current critical mass, it is now easier to introduce stronger compliance and enforcement mechanisms.

The following recommendations can be made with regard to the commercial viability of trustmark schemes:

1. All three trustmark schemes that provided information on their revenue generated during the start-up phase obtained their revenue from a private source. Also in the operational phase, the vast majority of revenue stems from a private source. At least three and a maximum of six of the selected trustmark schemes have proven to be commercially viable. Therefore, it is not recommended to financially support trustmark-scheme organisations in their operations with public means.
2. However, when looking at the critical success factors indicated by the trustmark schemes themselves, the creation of awareness could contribute to their commercial viability. It is recommended to allocate public means to awareness-raising activities, while more emphasis could be given on businesses rather than consumers. Ideally, the business and consumer organisations play a leading role in this. Project subsidies can be awarded to organisations that enrol awareness-raising activities, such as organising workshops, website, newsletters, articles in members' magazine, free-press, awareness questionnaires, or (online) awareness campaigns.
3. With any new trustmark scheme, it is recommended to subsidise the creation of a code of conduct (15% of start-up costs) through public means. This does not only lead to a cost reduction in the start-up phase, but also shortens the start-up period. This may be done by directly subsidising the creation of a code, for example via a project subsidy. Alternatively, public means could be used to allocate experts who provide assistance or guidance in the creation of the code of conduct.

Overall conclusions and recommendations

Converging and diverging issues resulting from the previous analyses were identified. As such, a synthesis was made of the business and consumer perspectives, the legal analysis and the commercial viability analysis. The additional ensuing conclusions and recommendations are listed in the table below.

Table 0.1
Overall conclusions and recommendations

	Consumers	Business	Legal Criteria	Commercial	Recommendation
Elaboration	Involvement is important Consumers believe that public endorsement is important	Involvement is important	Legitimacy (64.44%) is determined by a number of factors, notably consumer involvement and public endorsement	Not applicable	Active intervention of all the different stakeholders, notably consumer and business associations Set EU minimum standard for trustmark scheme quality
Order procedure	Very important	Very important	Confirmation process (68.89%)	Not applicable	Added value of Codes: - Clear, easy to understand and transparent manner of information. - Error detection also in relation to consent errors.
Applicable law	Law of residence	Law of place of establishment	Applicable law (53.33%)	Not applicable	Reconcile: - Country of Origin principle - Consumer protection legislation.
Dispute resolution and enforcement	Very important	Very important	Pro-active monitoring (40.71%) Monitoring (49.44%) Enforcement (39.29%)	High enforcement costs (21% of operational budget)	Co-operation between schemes or outsourcing to pan-European structure (EEJ Net).
User fee dilemma	Not applicable	Low user fees or free of charge	Not applicable	High user fees	No government intervention required.

Table of content

1	INTRODUCTION	16
2	RESEARCH DEFINITION	17
2.1	RESEARCH QUESTIONS.....	17
2.2	METHODOLOGY.....	17
2.3	SCOPE.....	19
3	BUSINESS AND CONSUMER ANALYSIS	20
3.1	INTRODUCTION.....	20
3.1.1	<i>Target groups</i>	20
3.1.2	<i>Finding respondents for the online questionnaire</i>	20
3.1.3	<i>Breakdown of the valid responses</i>	21
3.1.4	<i>Presentation of the results</i>	21
3.2	THEORETICAL FRAMEWORK ON CRITICAL SUCCESS FACTORS.....	22
3.3	BUSINESS AND CONSUMER ACCEPTANCE ANALYSIS.....	22
3.3.1	<i>Code of conduct</i>	22
3.3.2	<i>Enforcement of the code of conduct</i>	24
3.3.3	<i>Organisational aspects of the trustmark scheme</i>	26
3.4	BRAND-VALUE ANALYSIS.....	28
3.5	CONSUMER EXPERIENCE ANALYSIS.....	30
3.5.1	<i>Presentation of the trustmark</i>	30
3.5.2	<i>Expected effects of a trustmark scheme</i>	32
3.5.3	<i>Extra comments</i>	33
3.6	CONCLUSIONS AND RECOMMENDATIONS.....	34
4	LEGAL ANALYSIS OF TRUSTMARK SCHEMES	38
4.1	INTRODUCTION.....	38
4.2	METHODOLOGY.....	38
4.3	LIST OF CRITERIA ACCORDING TO THE LIFE CYCLE.....	43
4.4	TABLE OF “MUST-HAVE” CRITERIA.....	48
4.5	FINDINGS AND TRENDS.....	49
	<i>General observations</i>	49
4.5.1	<i>Phase 1: Elaboration of the trustmark scheme</i>	53
4.5.2	<i>Phase 2: Information on the trustmark scheme’s functioning</i>	58
4.5.3	<i>Phase 3: Participation in the trustmark scheme</i>	61
4.5.4	<i>Phase 4: Code of Conduct</i>	64
4.5.5	<i>Phase 5: Proactive monitoring</i>	77
4.5.6	<i>Phase 6: Complaints procedure</i>	79
4.5.7	<i>Phase 7: Enforcement</i>	82
4.5.8	<i>Phase 8: Relationships with protagonists</i>	84
5	COMMERCIAL VIABILITY ANALYSIS ON TRUSTMARK SCHEMES	87
5.1	INTRODUCTION.....	87
5.2	THEORETICAL FRAMEWORK ON TRUSTMARK-SCHEME BUSINESS MODELS.....	87
5.2.1	<i>Baseline organisation models</i>	87
5.2.2	<i>Financial model</i>	87
5.3	BUSINESS MODELS USED IN PRACTICE.....	90
5.3.1	<i>Organisation models in practice</i>	90
5.3.2	<i>Start-up phase</i>	91

5.3.3	<i>Operational phase</i>	94
5.4	CRITICAL SUCCESS FACTORS ACCORDING TO TRUSTMARK SCHEMES.....	97
5.5	CONCLUSIONS AND RECOMMENDATIONS	98
6	OVERALL CONCLUSIONS AND RECOMMENDATIONS.....	102
6.1	ELABORATION OF THE TRUSTMARK SCHEME	102
6.2	PUBLIC ENDORSEMENT – PUBLIC SUPPORT.....	102
6.3	ORDER PROCEDURE	102
6.4	COMPLAINTS PROCEDURE, DISPUTE RESOLUTION AND ENFORCEMENT	103
6.5	APPLICABLE LAW	103
6.6	THE USER FEE DILEMMA.....	103

1 Introduction

In 2000, the European Commission launched an initiative to strengthen consumer confidence in e-commerce. This work focussed on the role and effectiveness of trustmarks in the European e-commerce market place.

Following a joint project by stakeholders, a draft set of European trustmark requirements was produced by the Federation of European Union Employers' Federations (UNICE) and de Bureau Européen de Consommateurs (BEUC). These requirements aim at setting a high (but voluntary) standard for e-commerce trustmarks and include proposals for certification of the trustmarks and monitoring of their compliance with the requirements.

At the same time, evidence in the market place suggests that trustmarks have difficulties both in achieving brand recognition by consumers and in becoming commercially viable and sustainable operations. Therefore, it would be useful to have more in-depth information about the role and potential of trustmark schemes in the e-commerce marketplace in the European Union.

On 22 December 2003 the ECP.NL/CRID consortium were awarded a contract by the European Commission (DG SANCO) to analyse and define the common characteristics of trustmarks and webseals in the European Union. The work started in January 2004 and ended in December 2004. This document is the final report.

The first chapter of the report outlines the research definition. The business and consumer acceptance analysis is discussed in the second chapter. The next chapter goes into detail on the legal analysis of trustmark schemes, while the fourth chapter deals with the commercial viability analysis of trustmark schemes. The report ends with overall conclusions and recommendations.

2 Research definition

After defining the research questions, this chapter defines a research methodology with four distinct phases. A more detailed methodology is defined for the third phase. It also includes the proposal's work packages and their deliverables. Finally, the scope of the research is discussed.

2.1 Research questions

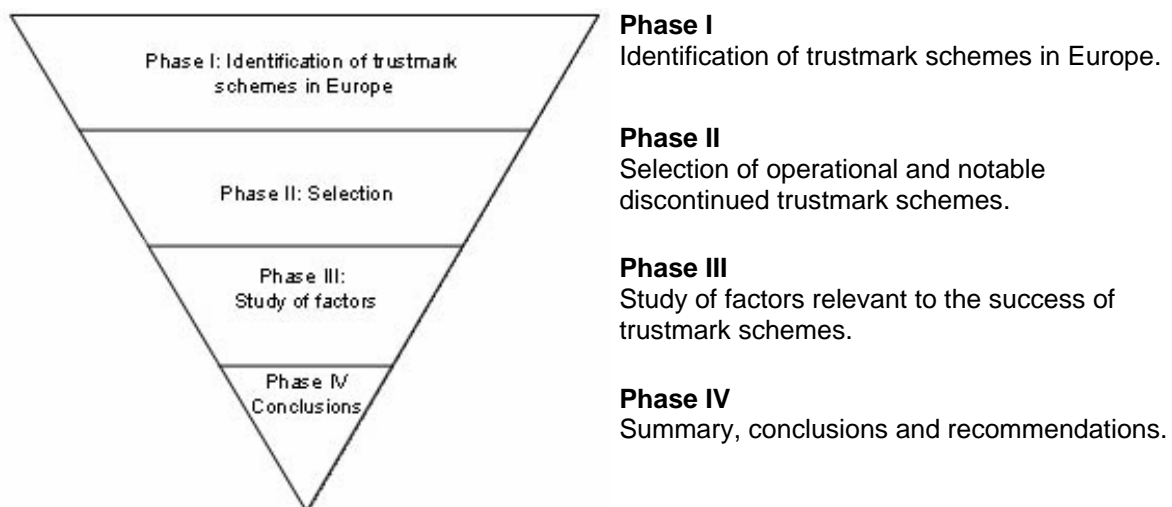
The purpose of this research is to obtain an analysis of the e-commerce market from the perspective of trustmark schemes. This analysis should allow drawing conclusions:

- § as to the usefulness of trustmarks for consumers, regarding the extent to which such trustmarks contribute to strengthening consumer confidence;
- § about the extent to which trustmarks are commercially viable operations, or can be made viable;
- § as to the conditions under which trustmarks would gain most acceptance from consumers and businesses alike. This would mean in particular issues related to independence, monitoring and enforcement, but also the administration and management of such operations, and their costs;
- § on the extent to which trustmarks benefit different types of e-merchants (major enterprises as opposed to SMEs), and to which extent they substitute (or have potential to substitute) brand recognition on the e-commerce market.

2.2 Methodology

In order to perform a detailed analysis of the e-commerce market from the perspective of trustmark schemes, a research approach was proposed that starts of with a broad scope, which narrows, but expands in depth as the project advances. The research approach can be divided into four distinct phases, which are described in the research approach outline (Figure 2.2.1).

Figure 2.2.1
Research approach outline



For the third phase of the research, the proposal includes a methodological approach which groups the questions posed by the Commission, while identifying the separate actors involved. This not only creates a more comprehensive overview of the work, but also allows a logical breakdown in separate work packages (see Figure 2.2.2).

Figure 2.2.2
Research methodology for phase III

Actors					
	Businesses	Consumers	Trustmark schemes	ECP.NL/CRID (Desk Research)	
A	<i>Survey: the subjective experience of trust²</i>	<i>Survey: the subjective experience of trust³</i>		Objective trustmark benchmark and legal analysis	WP2
B			Survey	Business models analysis	WP3
C	Survey	Survey			
D	Survey	<i>Survey⁴</i>			
	WP5	WP4			

- A) Consumer confidence and benchmarking the Guidelines versus Trustmarks
- B) Commercially viability of trustmark schemes
- C) Acceptance of trustmark schemes amongst businesses and consumers
- D) Brand-value analysis

The work can be broken down into work packages, for which deliverables can be defined. An overview of the work packages and deliverables is presented in Table 2.2.1.

² Initially, this survey was not included in the proposal as part of WP5. After setting up the online questionnaire, it appeared to be easy to include this survey and to allow a comparison with the business perspective with regard to the subjective experience of trust.

³ The original proposal includes an online survey directly aimed at consumers. During the kick-off meeting, the Commission and the ECP.NL/CRID consortium decided not to include this in the work of WP4 because the expectations about the quantity and quality of the response were too low.

⁴ Initially, this survey was not included in the proposal as part of WP4. During the kick-off meeting, the Commission and the ECP.NL/CRID consortium jointly decided to include this in the work because it would allow a comparison with the business perspective with regard to brand perception.

Table 2.2.1
Overview of work packages and deliverables

Work package	Deliverable
WP1: Identification and selection	Overview of trustmarks in the EU, including new member states, and acceding states.
WP2: Benchmarking	Written report
WP3: Business-model analysis	Business-model analysis report
WP4: Consumer survey	Questionnaire and results of questionnaire
WP5: Business survey	Questionnaire and results of questionnaire
WP6: Final analysis	Final Report, WP's 1-5, Analysis and Recommendations
WP7: Project management	Workplan, meetings, reports

2.3 Scope

The geographical scope of the research is the European Union. For the purpose of the analysis, the following trustmark schemes have been identified and selected (deliverable WP1): Confianza Online, Euro-label, Luxembourg e-commerce certified, Thuiswinkel, Trusted shops, TrustUK, Web Trader, WebTrust and QWeb. Annex 1 includes a list of selected trustmark schemes and respondents.

Although the geographical scope of the analysis is the European Union, the *BBBOnline* initiative that currently operates in Northern America is added to this list. *BBBOnline* has proven to be one of the leaders in this field from which best-practice business models can be leveraged to the research, in particular within the context of the business-model analysis (WP2).

3 Business and consumer analysis

3.1 Introduction

The goal of this part of the study is to identify which aspects of a trustmark scheme would contribute to its success. They are called “critical success factors” or “CSFs”.

3.1.1 Target groups

Two target groups have been identified to establish the critical success factors for trustmark schemes. First, the businesses that would or would not be interested in joining a trustmark scheme in order to increase confidence of potential buyers in their online shops. Second, the consumers who would or would not be convinced that a certified online shop is trustworthy.

Because the scope of the research included 25 countries and answering the questions required some knowledge about the subject, the decision was made to contact representatives of businesses and consumers in EU countries and ask them to answer the questionnaire thinking of the people they represent.

3.1.2 Finding respondents for the online questionnaire

The following organisations were contacted: BEUC⁵, UNICE⁶ and UEAPME⁷. They in turn contacted their members and asked them to respond to the questionnaire. A letter of approval from the European Commission was included with the invitation.

The questionnaire was launched on the 3rd of May 2004. The first invitation resulted in seventeen valid responses (seven consumer and ten business representatives). Four of the business questionnaires were filled out by trustmark organisations. Those four responses were deleted. A reminder was sent after four weeks. No further consumer representatives and one business representative responded.

In September the effort was made to call all registered members of UEAPME (40), UNICE (40) and BEUC (39) based on the information provided on their websites. Not all organisations could be reached for different reasons⁸. Four business-representative organisations said they had no knowledge of e-commerce and couldn't fill out the questionnaire, while one even refused to co-operate.

This follow-up resulted in nineteen responses to the business questionnaire, but only ten were filled out properly. The other nine only filled out the first questions (concerning

⁵ Bureau Européen des Unions de Consommateurs. BEUC is the federation of independent national consumer organisations from the EU, accession and EEA countries.

⁶ Union des Industries de la Communauté Européenne. UNICE's members are the central national business federations of European countries.

⁷ Union Européenne de l'Artisanat et des Petites et Moyennes Entreprises. UEAPME is the employer's organisation representing the interests, at European level, of crafts, trades and SMEs in the whole of Europe.

⁸ Incorrect phone-numbers, no English, French, German, Spanish or Italian was spoken, repeatedly no response or answering machines.

organisation, e-mail address, etc.). There were eleven further usable results for the consumer questionnaire.

In October reminders were sent out to the organisations that hadn't responded yet and to the representatives who left their e-mail address but did not fill out the rest of the questionnaire. This yielded no extra response.

In total there were eighteen valid responses from consumer organisations and seventeen from business organisations.

3.1.3 Breakdown of the valid responses

The responding consumer organisations are from:

- § EU member states: Austria, Denmark, Germany, Greece (2), Ireland, Luxembourg, United Kingdom (2), Czech Republic, Cyprus, Hungary, Poland, Slovakia, Slovenia
- § Outside EU: FYR of Macedonia, Switzerland, Iceland

The responding business organisations are from:

- § EU member states: Austria, Belgium (2), Denmark, Finland, Italy (2), Luxembourg, Netherlands, Portugal, Czech Republic, Lithuania, Malta, Slovenia
- § Outside EU: Norway, Switzerland and Romania

These respondents represented:

- § Large businesses or large business organisations (5)
- § SMEs or SME organisations (4)
- § A combination or other (8)

3.1.4 Presentation of the results

In this chapter the results of the questionnaire are presented in tables. The tables contain a shortened version of the questions. The complete questions and introductions are included in annex 6 and 7.

Because the response is too low to process the results statistically they are presented in absolutes. The results only reflect the opinion of the responding organisations, not of all business or consumer representing organisations in Europe.

An analysis was made of the responses of large business representatives (5) versus SME representatives (4). Where the difference of opinion was large⁹ or otherwise interesting this is mentioned in the text.

⁹ More than 1 point difference between these specific respondents and the rest of the target group on a scale of 1 to 5

3.2 Theoretical framework on critical success factors

The basis for the identification of critical success factors (CSFs) for trustmark schemes was found in a combination of desk research and expert interviews. The identified categories are as follows:

- § Code of conduct
- § Enforcement of the code of conduct
- § Organisation of the trustmark scheme
- § Brand value
- § Website of the trustmark scheme
- § The trustmark logo
- § Expected results of trustmarks

All these factors are involved in the acceptance of trustmarks. The brand value and consumer experience of trustmarks have been highlighted separately in the analysis.

Most questions in the online questionnaire could be answered by scoring the importance of CSFs on a scale of 1 to 5. Other questions were multiple choice, open ended or were statements which the respondent could (dis)agree with.

3.3 Business and consumer acceptance analysis

3.3.1 Code of conduct

The code of conduct forms the core of a trustmark scheme. It specifies all the obligations of certified online shops, such as publishing certain information about the shop on its website, compliance with a dispute resolution procedure or a money-back guarantee.

§ The consumer perspective

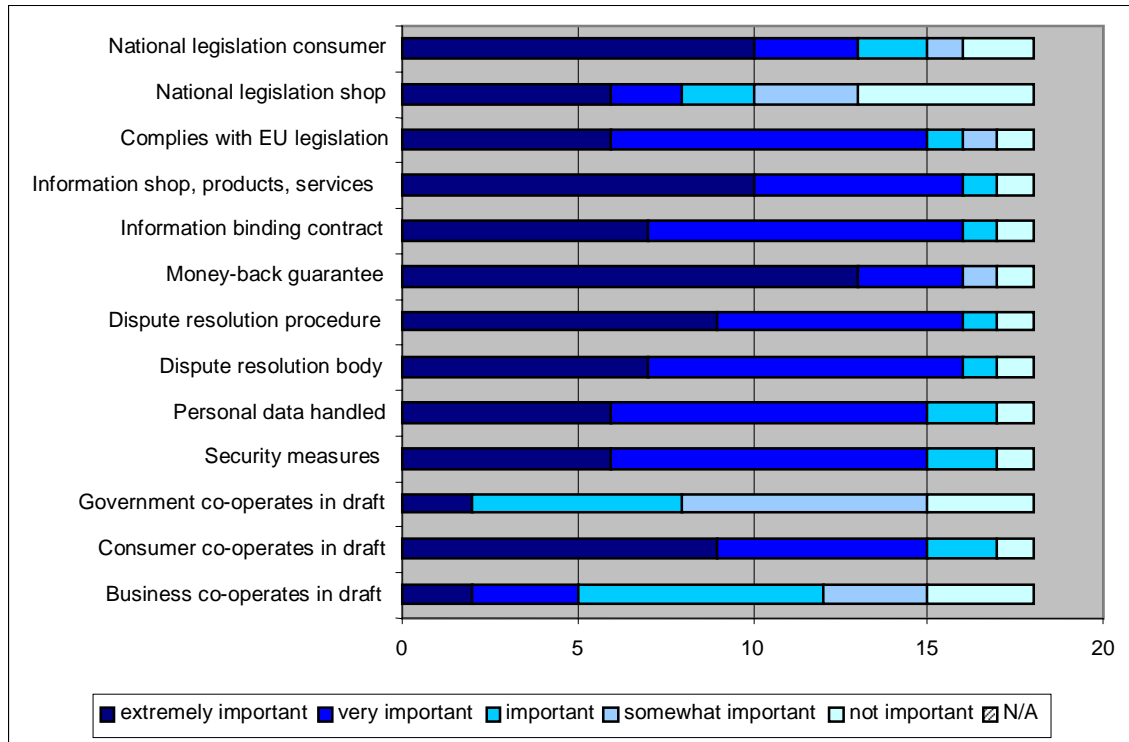
Most consumer representatives have indicated that it is at least very important that a code of conduct complies with European Union regulations and also with the national law of the country where the consumer lives.

The appointment of a dispute-resolution body and adoption of a dispute-resolution procedure seems to be critical. But most important for the success of a code of conduct is the inclusion of a money-back guarantee; thirteen out of eighteen respondents say this is “extremely important”.

According to the consumer representatives, the code of conduct must state what security measures are used by certified shops and how personal data of consumers is handled. It is just as important to state the procedure to enter into a legally binding contract. It is even more important to require that online shops publish certain information about themselves, their products and services on their website to enable consumers to make an informed choice.

The responding consumer organisations think that it is critical that consumer organisations are involved in the drafting of the code of conduct of a trustmark scheme. The influence of industry organisations and government on the content of the code is less important.

Table 3.3.1.1
CSF code of conduct – consumer perspective



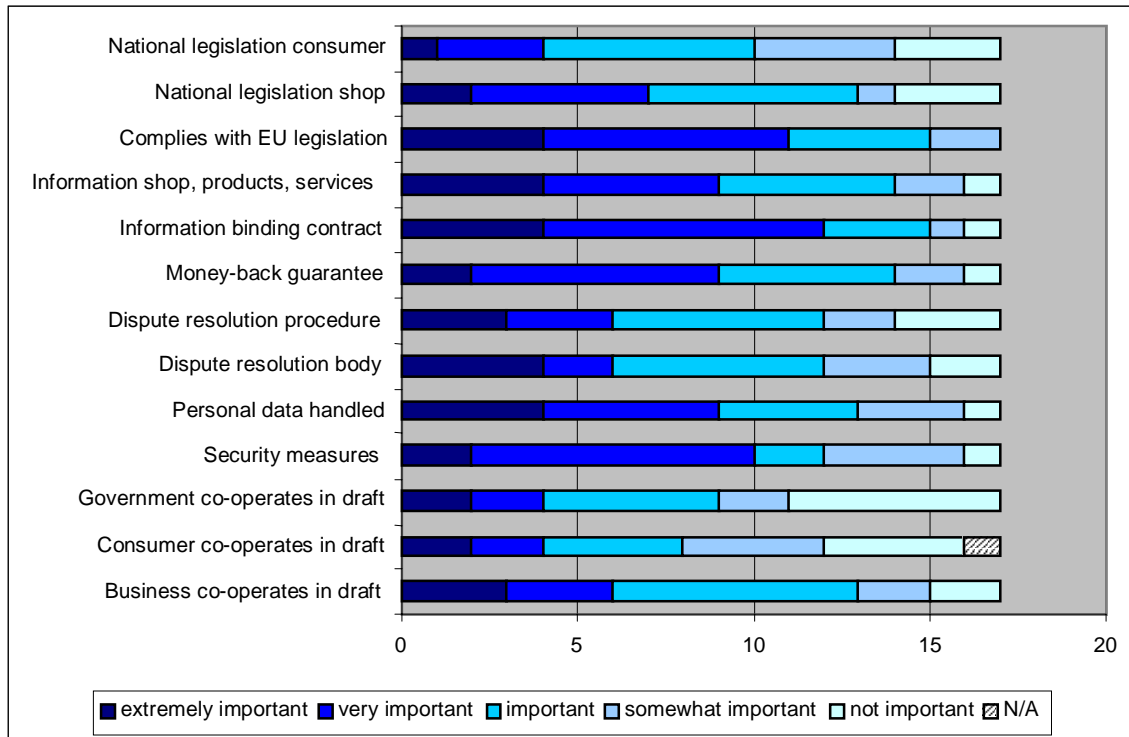
§ The business perspective

According to the majority of the responding business representatives it is very or extremely important that a code of conduct complies with EU legislation.

Twelve out of eighteen business representatives think it is at least very important that a code of conduct contains information about the procedure to enter into a legally binding contract.

More business representatives are of the opinion that it is more important that businesses have influence on a code of conduct than consumers or government have influence on it.

Table 3.3.1.2
CSF code of conduct – business perspective



3.3.2 Enforcement of the code of conduct

A trustmark-scheme organisation needs to know whether the shops that want to join the trustmark scheme comply with the rules laid down in the code of conduct. This can be brought about, for example, by requiring (regular) audits on different aspects of the code of conduct (preventive measures) or by assigning a dispute-resolution body that handles complaints (repressive measures).

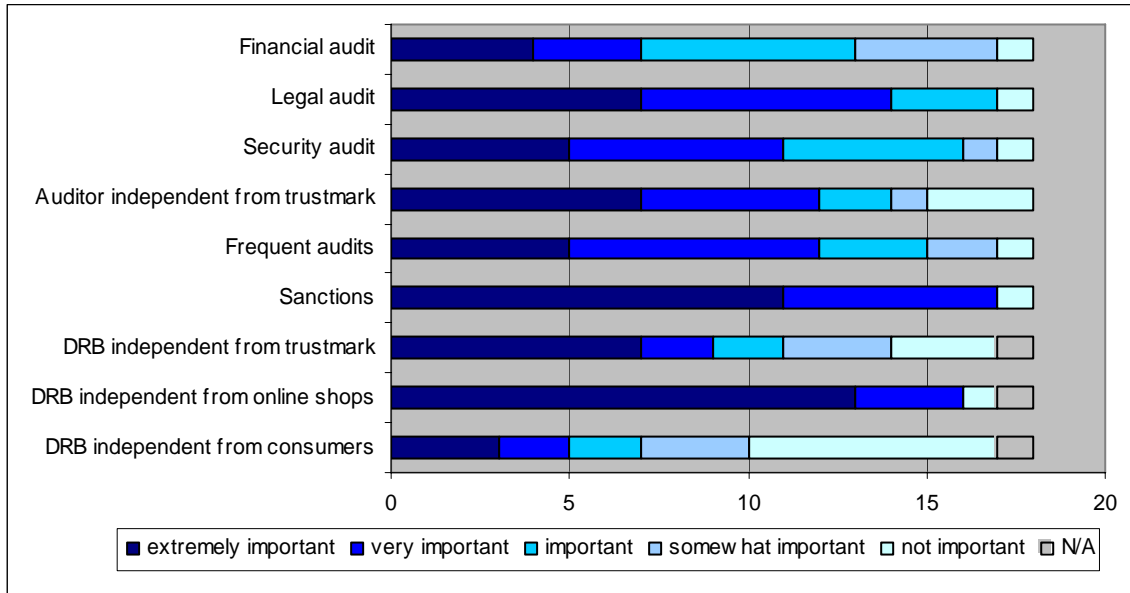
š The consumer perspective

According to the majority of the respondents it is at least very important that a trustmark scheme requires a legal and security audit and a little less important to require a financial audit. It is also important that the auditor is independent from the trustmark-scheme organisation and that audits are repeated.

All but one respondent think it is very or extremely important that a trustmark scheme can enforce compliance with the code of conduct, for instance by withdrawing the trustmark logo.

The consumer representatives feel that it is very important that the dispute-resolution body is independent from the online shops. Independence from the trustmark scheme is less important, while independence from consumer organisations is least important.

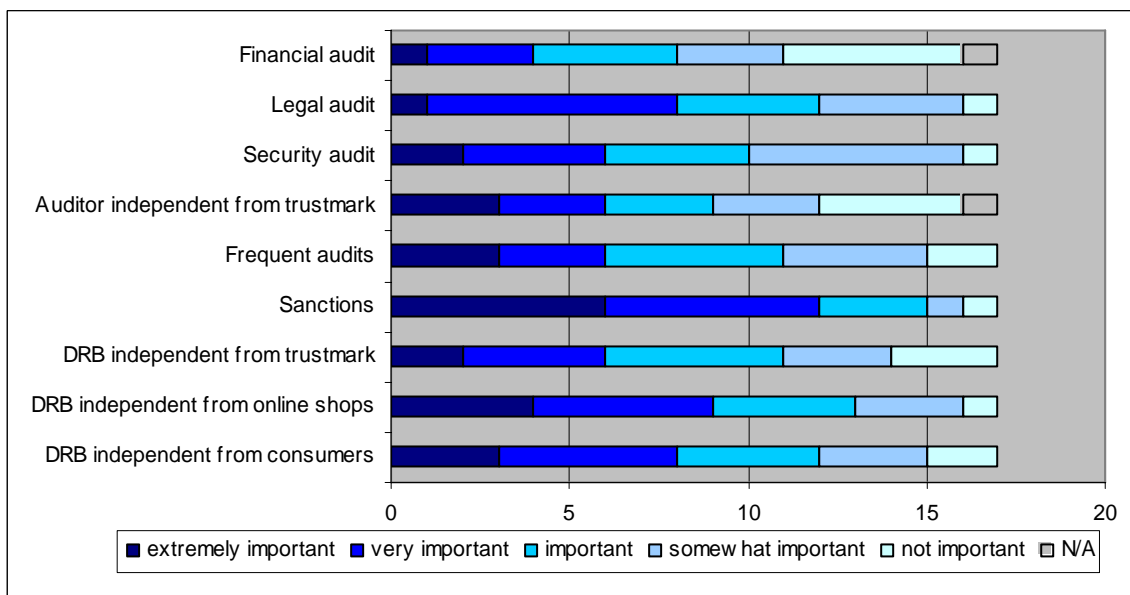
Table 3.3.2.1
CSF enforcement – consumer perspective



§ The business perspective

According to the responding business organisations legal and security audits are more important than financial audits.

Table 3.3.2.2
CSF enforcement – business perspective



Of the seventeen respondents in this category, twelve are of the opinion that it is very or extremely important that the trustmark scheme is able to apply sanctions when certified

shops do not comply with the code of conduct. Only one of the five organisations that represent only large businesses thinks sanctions are very or extremely important.

Most business representatives think it is important that a dispute-resolution body of a trustmark scheme is independent from online shops.

3.3.3 Organisational aspects of the trustmark scheme

The location of a trustmark-scheme organisation might be of influence on the acceptance of the trustmark. Should it be located near the consumer or the operator of the online shop? Also the representation of different interest groups might be important. For businesses that are the potential clients of the trustmark scheme some other factors might be important: what are the costs of joining and how complicated is the application procedure?

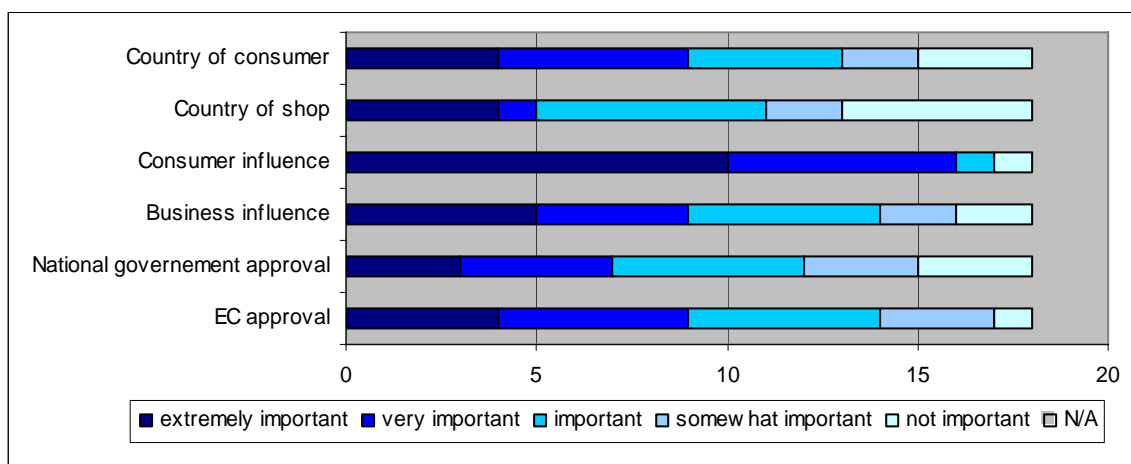
§ The consumer perspective

The responding consumer organisations seem to have a preference for the trustmark scheme to be located in the country where the consumer lives.

According to sixteen consumer representatives it is at least very important that consumers are represented in the trustmark-scheme organisation. Business representation is less important.

The responding consumer representatives think it is more important that the European Commission approves of a trustmark scheme than a national government.

Table 3.3.3.1
CSF organisational aspects – consumer perspective



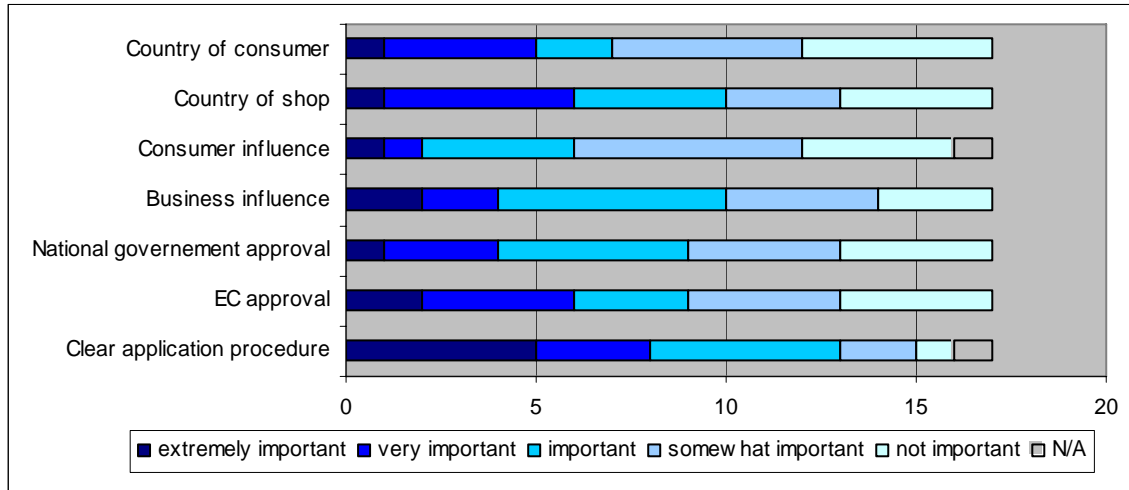
§ The business perspective

Business representatives seem to have a preference for the trustmark scheme to be located in the country where the certified online shops are based.

According to the business representatives (especially the organisations that represent SMEs) it is more important that businesses are represented in the trustmark-scheme organisation than consumers. They are less outspoken than the consumer representatives.

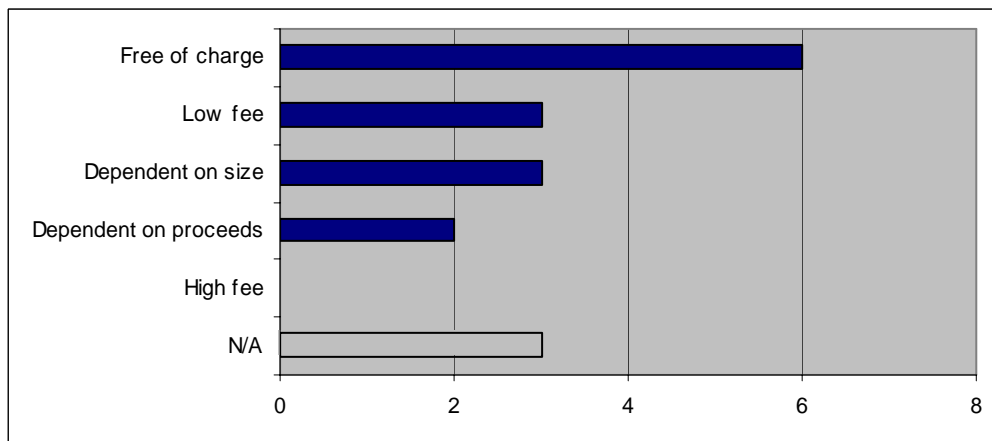
The respondents seem to slightly prefer European Commission approval of the trustmark scheme over national government approval.

Table 3.3.3.2
CSF organisational aspects – business perspective



Only eight of seventeen business representatives think it is at least very important for the success of a trustmark scheme that there is a clear application procedure for online shops that want to join¹⁰. Especially the organisations that represent only large businesses feel this is not particularly important. Still, this aspect is valued higher by this group of respondents than any other organisational aspect.

Table 3.3.3.3
CSF fees – business perspective



An extra question was added to the questionnaire for the business representatives to find out whether there would be a preference for the level of costs of joining a trustmark scheme. Most respondents think the companies they represent would want the trustmark free of charge, three of them represent SMEs. The next choice of the respondents is to have a fee dependent on the size of the company or their revenue. The rest thinks the fee should be

¹⁰ This question was only included in the questionnaire for business representatives.

low¹¹. Three respondents did not answer the question. No respondents indicated the annual fee should be high¹².

One of the respondents who did not answer this question explained that trustmark schemes should be market based. “The fees should be allowed to find appropriate levels on the markets, based on the added value that the trustmark brings the online shop and what the online shop is ready to pay for it”.

3.4 Brand-value analysis

Having a valued brand is important for a trustmark scheme because it will raise both business and consumer confidence in e-commerce and therefore contribute to the success of the trustmark scheme.

The questions concerning brand value of trustmarks can be divided into several aspects:

- § Is it important that the trustmark starts out with a valued brand?
- § Does the brand of certified online shops add value to a trustmark brand?
- § Does joining a trustmark add value to the brand of the certified online shops?
- § Does the quality or the quantity of the online shops that join a trustmark influence the brand of the trustmark scheme?

The perception of the logo of a trustmark scheme is dealt with in paragraph 3.5.1.

§ The consumer perspective

According to fourteen responding consumer representatives it is at least very important that the trustmark scheme is operated by an organisation with a well-known brand. This is somewhat more important than the brands of the certified online shops.

The respondents think that it is more important to consumers that a trustmark scheme has certified a large quantity¹³ of online shops than that the shops combined have a large market share¹⁴. Trusted Shops is an example of a trustmark scheme that certified a large quantity of shops (900 certified online shops). Luxembourg e-commerce certified, for example, has certified only six online shops. It will help though, according to the consumer organisations, if the certified shops are well-known to the consumers.

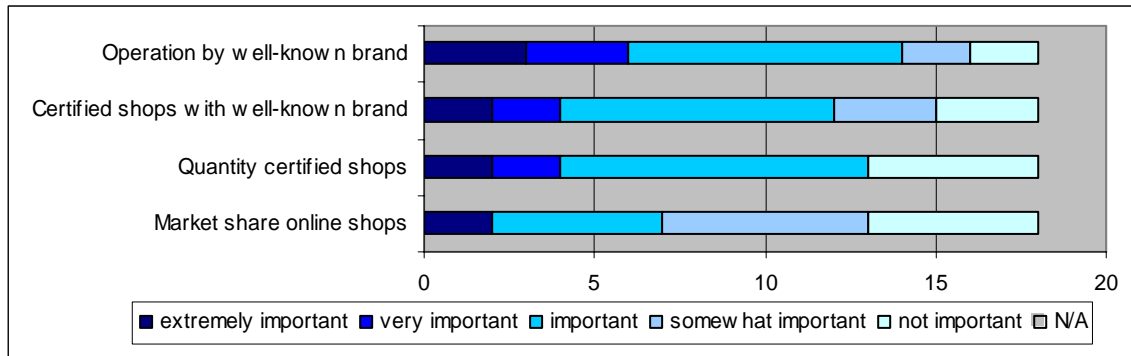
¹¹ As for instance Trusted Shops, that has a maximum annual fee of 1,200 Euros.

¹² As for instance Thuiswinkel.org, that has an annual fee between 1,300 and 29,000 Euros.

¹³ For the purpose of this analysis defined as “more than 100 shops”.

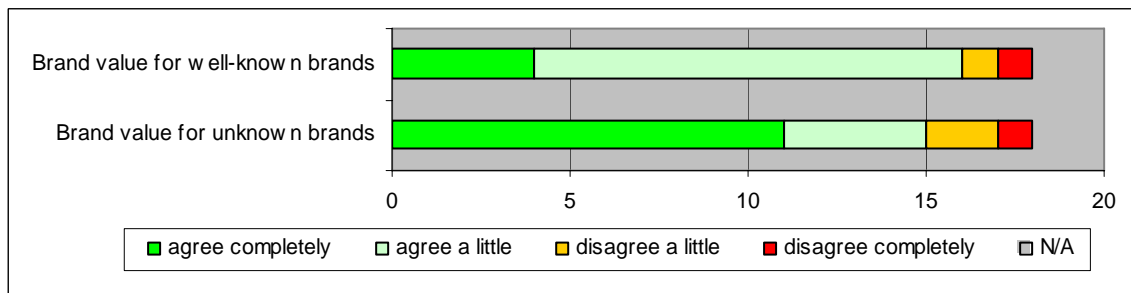
¹⁴ For the purpose of this analysis defined as “more than 75% of the online business to consumer market”.

Table 3.4.1
CSF brand value – consumer perspective



The consumer representatives think that joining a trustmark scheme will add brand value to all businesses, although the added value for unknown brands is larger.

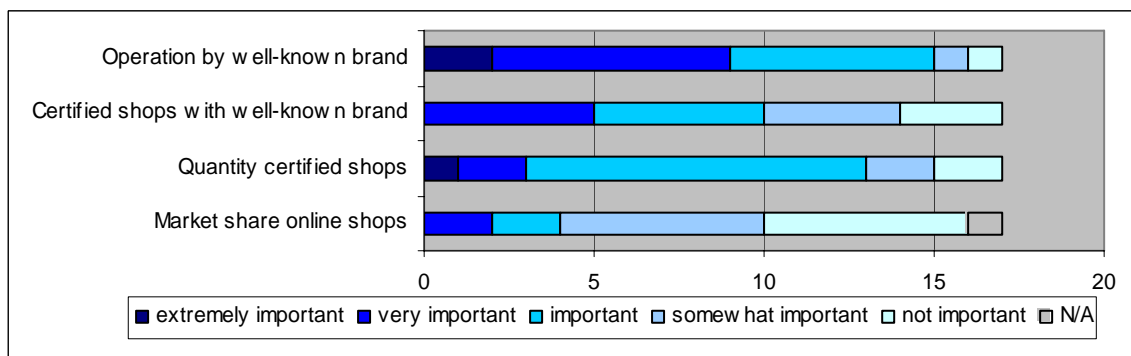
Table 3.4.2
CSF added value – consumer perspective



§ The business perspective

According to the business representatives, the brand of the operator of the trustmark is more important than the certification of online shops with well-known brands. There is no representative of large business organisations that finds the brand of the operator very or extremely important.

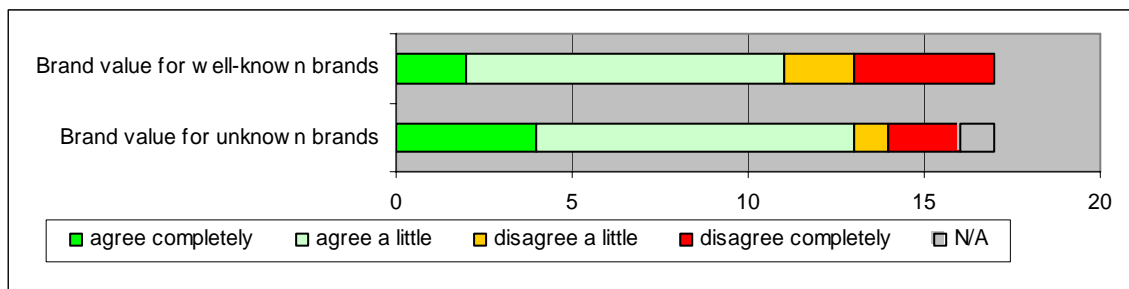
Table 3.4.3
CSF brand value – business perspective



The business representatives feel that it is important for a trustmark scheme to certify a lot of online shops. Their combined market share is much less important.

The majority of the business organisations that responded find that joining a trustmark scheme adds some value to online shops. The effect for unknown brands is a bit larger than for well-known brands. They are less positive about the added value of joining a trustmark than the consumer organisations.

Table 3.4.4
CSF added value – business perspective



§ Large businesses vs. SMEs

When comparing their opinions on the added brand value, large business representatives and SME representatives respond about the same. Three out of five large business representatives agree a little with both statements, two disagree completely. Three SME representatives think joining a trustmark scheme adds value to both well-known and less-established brands, one thinks this does not happen.

3.5 Consumer experience analysis

Trust is a subjective notion which is very hard to measure. For the purpose of this analysis the following aspects were identified:

- § The content of the trustmark's website
- § The logo of the trustmark
- § The language of the trustmark's website
- § The expected impact of trustmarks on consumers

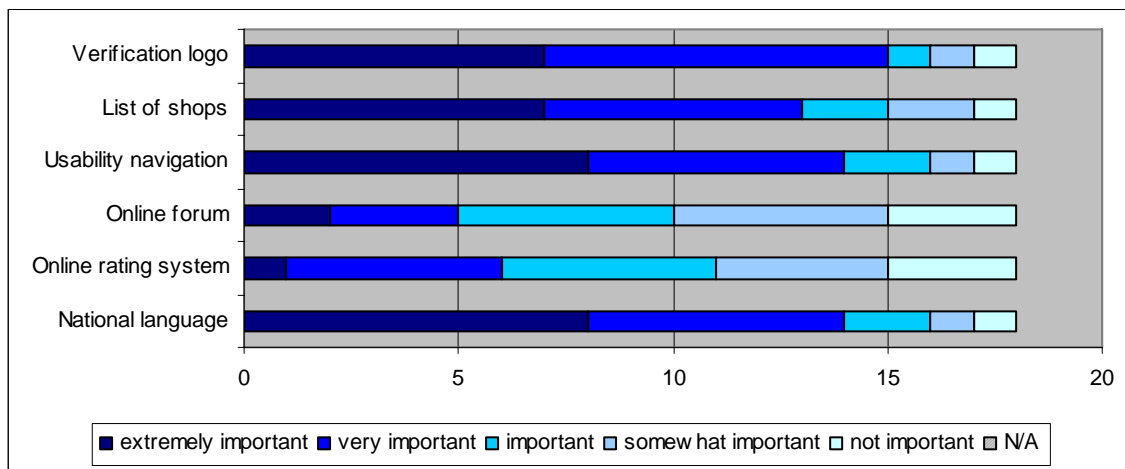
3.5.1 Presentation of the trustmark

§ The consumer perspective

Logo - The majority of the respondents from consumer organisations state that the shape of the logo should be a combination of a logo and a text. Most would like the design of the logo to be related to the internet, second are "related to shopping" and "modern". Half of the respondents indicate that they prefer the logo to be displayed in the menu on the left side of the online shop's website, which stays visible throughout the visit of the site. Second best was placement in the top bar (also visible throughout the visit of the site).

Website - According to the majority of respondents from consumer organisations it is at least very important that the website of a trustmark scheme offers a list of all certified shops. Also, it is at least very important that the consumer can click on the logo that is displayed on the certified website and be redirected to a website of the trustmark scheme that verifies the certification of this online shop. Fourteen representatives of consumer organisations say the usability of the website is very or extremely important. An online rating system and/or forum on which consumers can share their opinion about the service of certified shops is less important.

Table 3.5.1.1
CSF website – consumer perspective



Language - Most consumer representatives think it is very or extremely important that the trustmark scheme communicates with consumers through their own language. If they had to choose another language it would be English¹⁵. But would the consumers be able to understand the information on the trustmark scheme’s website if it was in English? Three representatives think most consumers in their countries would not, nine think they would and two even think it would make no difference for the consumers whether it was English or their own language.

The consumer representatives found it hard to choose between the options to use informal but simplified language or formal but correct language on the trustmark scheme’s website (both 50% of the respondents).

§ The business perspective

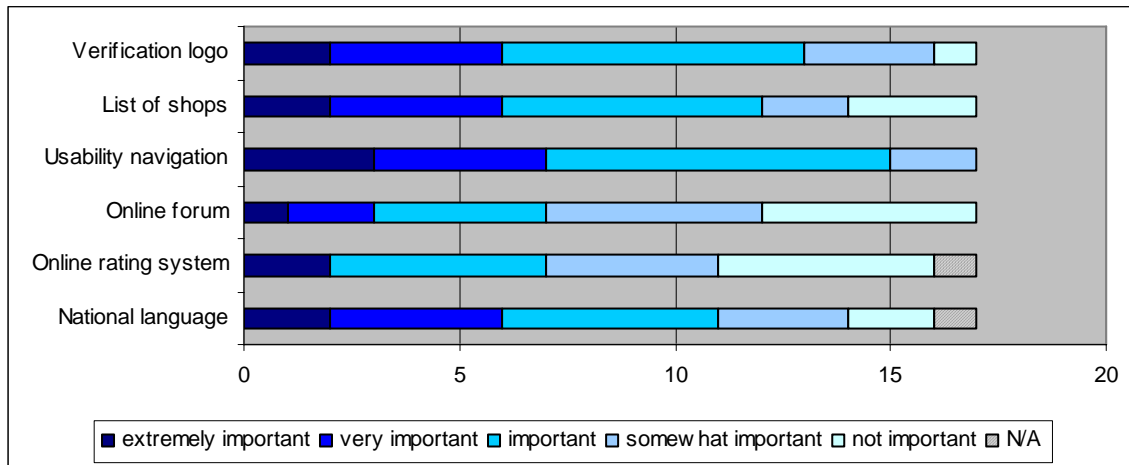
Just in case it might yield interesting information we asked the business representatives the same questions about the subjective experience of a trustmark, but now from the point of view of the companies they represent. The results are listed below.

Logo - The majority of the respondents from business organisations states that the shape of the logo should be a combination of a logo and a text. Most would like the design of the logo to be related to the internet, second are “conservative” and “modern”. Most respondents prefer the top bar as location for the trustmark seal. Second came the menu bar at the left or right of the website’s homepage.

¹⁵ According to fourteen of the fifteen respondents from countries where English is not the official language

Website - The business organisations that responded think that a trustmark scheme's website should have good navigation. A list of certified shops and the possibility to verify the logo of the trustmark on the website of an online shop are more important than an online forum or rating system.

Table 3.5.1.2
CSF website – business perspective



Language - For the large businesses in Europe it seems to be less important that the trustmark scheme communicates in their national language than for the consumers and SMEs. Asked what other language than their national language the companies in their country would prefer, all business representatives answered: "English". Of the seventeen respondents five think the companies in their country would not be able to understand the information if it were in English, though three think the companies would still have some trust in the trustmark scheme. Twelve of the seventeen respondents think the companies in their countries are able to understand English well enough.

Of the respondents nine indicated that they would prefer the use of informal but simplified language on the trustmark scheme's website. Four of them represent SMEs. Eight respondents prefer formal but correct language. Like the consumer organisations, the opinions of the business organisations are divided.

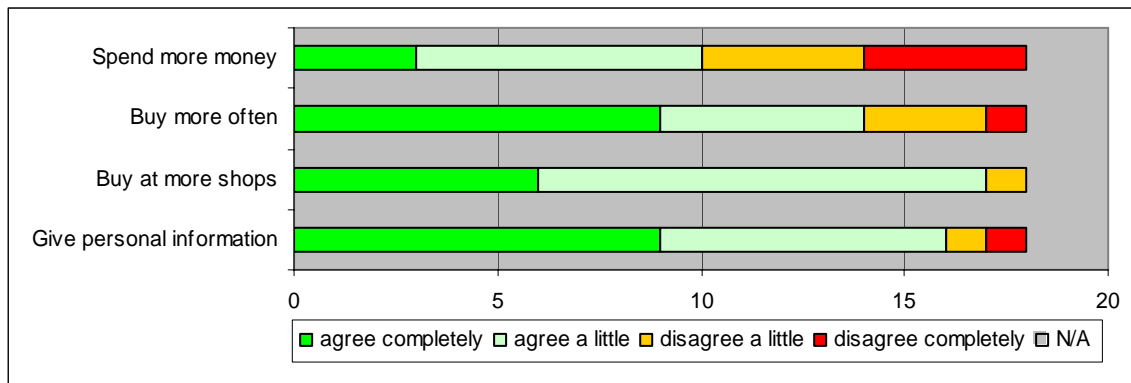
3.5.2 Expected effects of a trustmark scheme

The main reason for developing a trustmark scheme is to increase consumer confidence in e-commerce websites. Several possible effects of trustmark schemes were submitted to consumer and business representatives in Europe to find out whether they feel this goal is reached.

§ The consumer perspective

According to the consumer representatives, the largest effect of a trustmark scheme is that consumers will be more willing to leave personal information on a website of a certified shop. In terms of online shopping, they feel that it is more likely that consumers will buy online more often and at different shops than spend more money online.

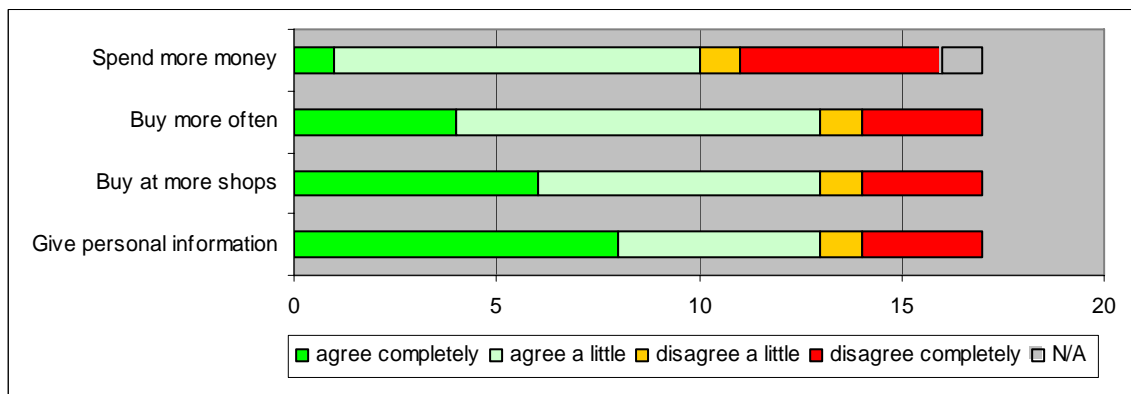
Table 3.5.2.1
Effects – consumer perspective



§ The business perspective

According to the business representatives, the overall impact of a trustmark scheme is less than the consumers think. The biggest effect would be that buyers would be more willing to give their personal information to certified online shops.

Table 3.5.2.2
CSF effects – business perspective



3.5.3 Extra comments

At the end of the questionnaire respondents were given the opportunity to comment on the subject or the questionnaire itself.

§ Consumer organisations

Three respondents of the consumer organisations noted that the questions were difficult to answer. The first noted that concrete circumstances are sometimes very important for the success of a trustmark. The second said that consumers might want to start a court procedure instead of going through a dispute-resolution procedure (this is always possible, but it was not stated explicitly in the questionnaire). The third stated that the questions about applicable law were difficult to answer because the code needs to be flexible enough to work internationally, also outside the EU.

Last open response of a consumer representative is that there are too many different trustmark schemes now, which confuses consumers. There should be a uniform trustmark scheme through the co-operation of industry, trade, consumers and the European Union.

§ Business organisations

A business representative stated that “some of the questions are based on the idea that “e-business” is something very different from “classical business” and that it thus requires a special approach and special regulation. I do not share this approach and I am not sure that trustmarks can bring any value into the business of these days”.

3.6 Conclusions and recommendations

§ Introduction

In this chapter the results were presented of a questionnaire that strived to identify the critical success factors (CSFs) for the acceptance of trustmark schemes by businesses and consumers in Europe.

In this last paragraph the most important CSFs overall are displayed. The respondents were asked to rate the CSFs on a scale from 1 to 5¹⁶. In the tables below the mean score per target group (business and consumer representatives) was used to create a top-10.

§ General conclusions

When evaluating the response to the online questionnaire the following conclusions can be drawn about the general opinion of the target groups:

1. Consumer representatives in general value the critical success factors much higher (very important) than the business representatives (important)
2. The response of business organisations to the online questionnaire (21%) is much lower than the response of consumer organisations (46%)
3. Based on the telephone conversations with European business organisations the level of knowledge of and enthusiasm about trustmark schemes for online shops seems low

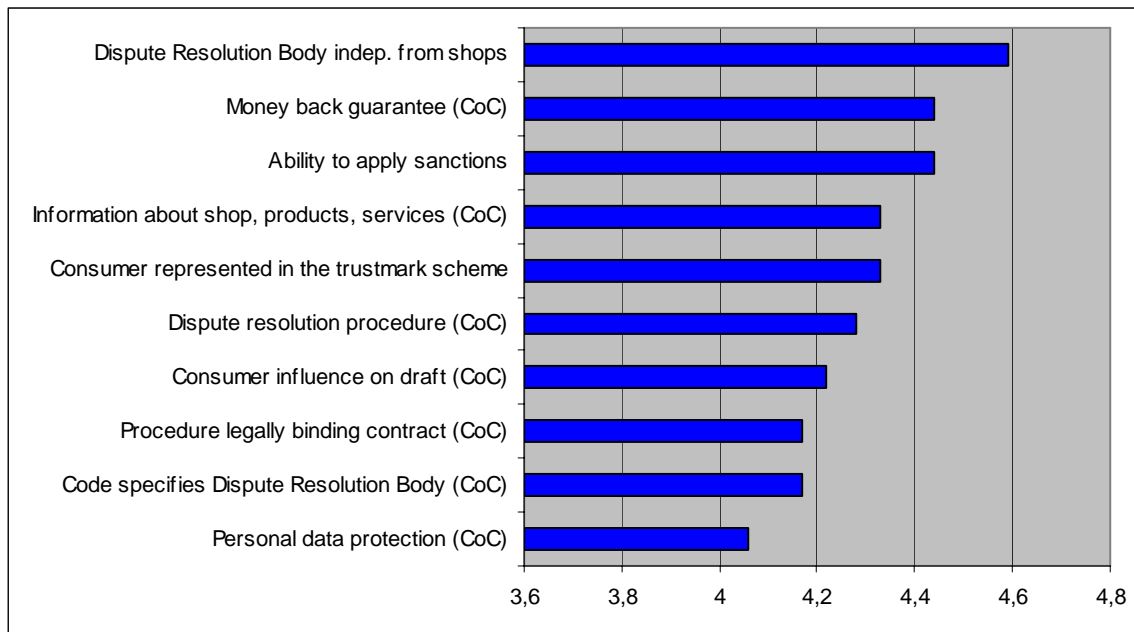
This indicates that consumer organisations feel the need for self-regulation in e-commerce, but the awareness in business organisations is relatively low.

§ The critical success factors for consumer organisations

The table below shows the top 10 critical success factors according to the consumer-organisation representatives. Most of these high-ranking CSFs concern the code of conduct (CoC). Also the enforcement of the regulations of the trustmark scheme is very important; the Dispute Resolution Body should be independent from the online shops and the trustmark scheme should be able to apply sanctions when certified shops do not comply with the code of conduct.

¹⁶ 1 = not important, 2 = somewhat important, 3 = important, 4 = very important and 5 = extremely important

Table 3.6.1
Top 10 CSF – consumer perspective



§ The critical success factors for business organisations

Table 3.6.2 shows the overall ranking of critical success factors by the business representatives. Half of the top 10 CSFs concern the content of the code of conduct (CoC). They find the ability to apply sanctions most important. It also seems to be important for businesses to offer a clear application procedure to online shops.

§ Critical success factors for all respondents

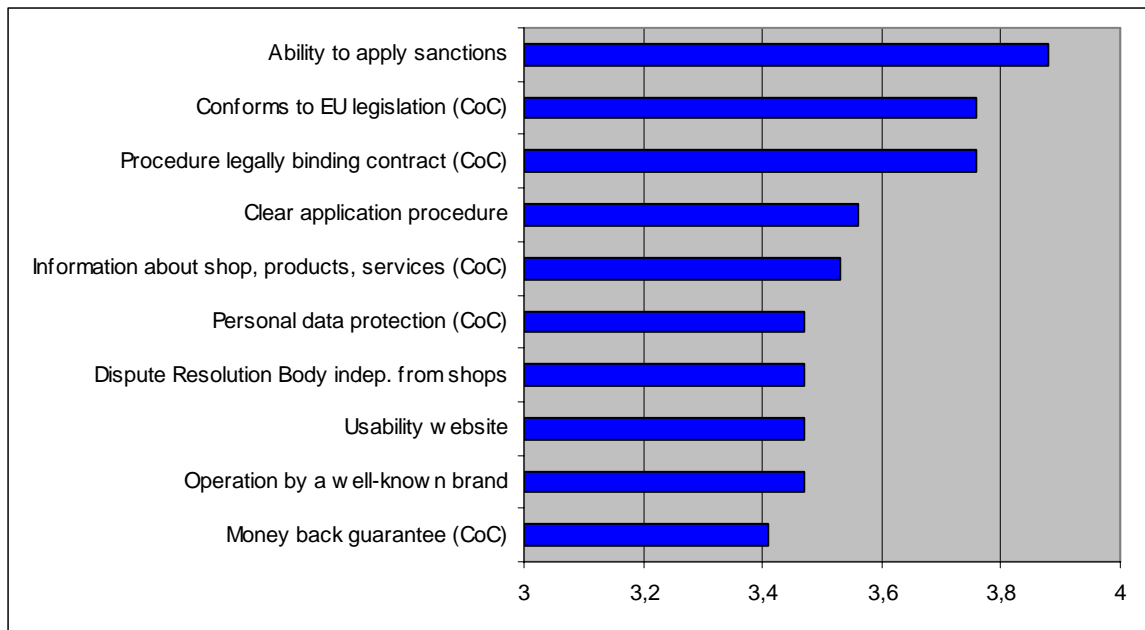
Table 3.6.3 presents the individual scores of all participants combined.

§ Recommendations on the acceptance of trustmarks

The recommendations to increase the acceptance of a trustmark are:

1. The most critical success factors are those that are contained in the code of conduct. Making sure the code complies with the applicable (EU) regulations is very important. This could be achieved by drawing up a model code of conduct at European level. Individual trustmark schemes can use it to save on legal expenses and uniformity of the codes might increase consumer confidence in trustmarks in general.
2. A “money-back guarantee” is supported by both consumer and business representatives. However, this guarantee is usually not given in a trustmark’s code of conduct. It might be wise for a trustmark scheme to include this benefit.
3. It is very important that a trustmark scheme has the power to take appropriate action when a certified shop does not comply with the code of conduct. It is advisable for a trustmark scheme to have more than one possible sanction (withdrawal of the logo).
4. The independence of the dispute resolution body should be ensured.
5. Trustmark schemes should be transparent. The acceptance of a trustmark scheme by potential clients (online shops) and consumers cannot be increased when they do not know what the benefits are.

Table 3.6.2
Top 10 CSF – business perspective

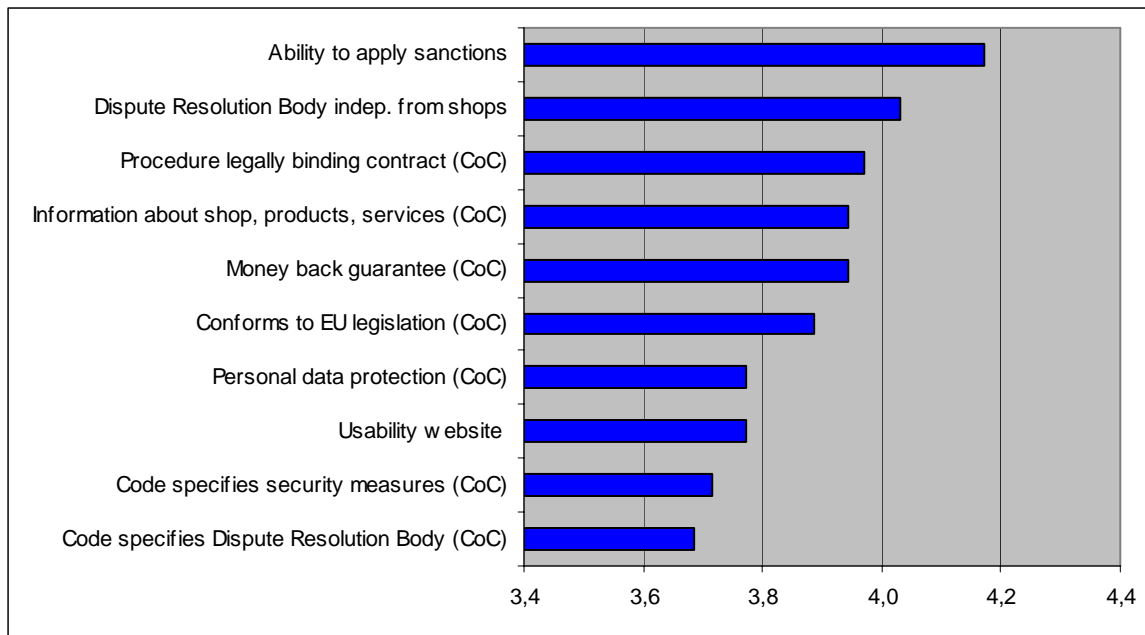


§ Conclusions and recommendations on brand value

From the results of the questions about brand value the following can be concluded:

1. It is important for the success of a trustmark that it has a strong brand. When an organisation which already has a strong brand starts a trustmark scheme this is easier to achieve than starting a new brand.
2. A small minority of the responding business representatives think joining a trustmark scheme adds substantial value to the brand of an online shop. Therefore, it is advisable for a trustmark scheme to research its influence on consumer confidence and show the results.

Table 3.6.3
Top 10 CSF – business and consumer combined



§ Recommendations on consumer experience

In the field of consumer experience the following recommendations can be made:

1. Consumers who take the effort to visit a trustmark's website should be able to find the information they look for easily. Investing in the usability of such a website is important.
2. According to the respondents, most consumers prefer to be communicated to in their own language. The best alternative is English, but using this language would decrease consumer confidence.
3. It may be effective to use a combination of informal, global information and formal, detailed information on the website of a trustmark scheme.
4. The respondents think the website of a trustmark should contain a list of certified online shops. It must be possible to verify certification by clicking on the logo of the trustmark on a certified website.

4 Legal analysis of trustmark schemes

4.1 Introduction

In this chapter the methodology and the projects' legal findings in relation to the selection of the legal benchmark criteria and the evaluation of these criteria are presented and commented.

The first section deals with the methodology used for the legal assessment of relevant criteria as derived from hard and soft sources of law¹⁷. Afterwards and from these different norms, two different sets of evaluation criteria have been elaborated. Whereas the so-called **must-have criteria** reflect the true legal added value of a trustmark scheme (section three), section two contains a list of all relevant general criteria, including the must-have ones. Eventually, based upon a vertical and horizontal evaluation of these two sets of criteria, we will identify some trends and formulate some closing remarks (section four).

4.2 Methodology

Trustmarks or seals of approval are currently one of the principal mechanisms for promoting consumer confidence in electronic commerce. Different types of organisations (usually referred as code owners) establish standards (codes of conduct) for conducting electronic commerce and certify that particular online businesses (code subscribers) meet those standards.

In order to be certified with a trustmark seal, a provider of information society services¹⁸ has to comply with the code of conduct of the trustmark organisation. The provisions of the code of conduct state how the subscriber must conduct its business and should, in best case, improve consumer confidence.

In this regard, one cannot deny that the code of conduct is the central element of such schemes. This paramount characteristic of codes of conduct can be the reason why most studies or surveys on trustmark schemes focus exclusively on this aspect. The examination of the content of the code of conduct allows assessing the level of the requirements imposed to the subscribers. Therefore, it allows to a certain extent the evaluation of the quality of a trustmark scheme. The code almost plays the role of a mirror that reflects the quality of the trustmark scheme.

However, it must be underlined that a multitude of legal criteria can be identified to assess the legal quality of a trustmark scheme. Even though codes of conduct are the core of most self-regulatory models, the quality of the trustmark scheme also depends on other criteria such as notably complaint handling, organisation, management and other scheme properties. In this respect, it must be underlined that an open and **functional definition** of the concept of scheme **codes of conduct** was adopted. Hereinafter, code of conduct shall

¹⁷ For a detailed overview of the project's methodology, normative sources or law, etc. reference is made to the annex of the present Final Report.

¹⁸ As defined by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998.

mean any document containing trustmark scheme obligations, principles or norms, this irrespective of their location on the website or formal label.

In order to avoid a too narrow basis of quality assessment, a **global approach** is advocated. An eloquent illustration of such a global approach are the **European Trustmark Requirements** (ETR) elaborated within the framework of the e-confidence initiative¹⁹. In addition to the requirements related to the content of the code of conduct, the European Trustmark Requirements address the following issues:

1. Transparency of trustmark schemes of consumers and business;
2. Accessibility and visibility of trustmark schemes of consumers and business;
3. Operation of trustmark schemes;
4. Assessment of applicants for trustmark schemes;
5. Monitoring system;
6. Enforcement system;
7. Technical security.

As demonstrated by this initiative, the content of the code is one of the relevant factors to benchmark the quality of a trustmark scheme, but not the only one. In this context, one has to take into account in the benchmark list a large range of factors concerning, on the one hand, the content of the code and, on the other hand, the other aspects of the organisation and functioning of a trustmark scheme.

To develop a model of trust that describes what legal factors affect the legal quality of a trustmark scheme, the legal analysis was not limited to a single benchmarking of the content of the selected trustmark schemes' codes of conduct. Instead, we did go further in adopting a more global perspective and covering the main aspects of this type of services.

For this reason, we elaborated a general list of criteria encompassing a number of criteria contained in various sources of regulatory instruments. The main regulatory instruments are the following²⁰:

§ Sources of Self-regulation (soft law)

- European Trustmark Requirements (ETR)
- Second draft principles for e-commerce codes of conduct (The E-Confidence Initiative Working Documents)²¹
- Global Business Dialogue on e-commerce Recommendations²²

§ Sources of EU law (hard law)

- The Directive on distance contracts
- The Directive on electronic commerce
- The Directive on personal data protection
- The proposal for the Directive on unfair commercial practices

¹⁹ UNICE-BEUC eConfidence Project, 22 October 2001, <http://www.euractiv.com/ndbtext/infosoc/econfidence.rtf>.

²⁰ See annexed WP 2: List of relevant criteria and regulations

²¹ Those principles are available on the 'eConfidence Forum' website, <http://econfidence.jrc.it>.

²² See the "Tokyo Recommendations" (Consumer confidence: Trustmarks), GBDe Conference, 13 and 14 September, 2001, Tokyo, Japan, <http://www.gbde.org/acrobat/trustmarks01.pdf>.

From these different normative sources, including dispositions of hard and soft law, the highest common factors or criteria were identified. This comparative process resulted in the elaboration of a list of more than 40 general selection criteria.

Afterwards, this general list was converted into a more functional synopsis. In function of the phases of the “**life cycle**” of a trustmark scheme, *i.e.*, from conception, dissemination to enforcement, different criteria were grouped and ordered in a more pragmatic and systematic manner²³.

For the purpose of the legal assessment, the following phases in the trustmark scheme’s life cycle were identified:

1. Elaboration of the trustmark scheme
2. Information on the trustmark scheme
3. Participation in the trustmark scheme
4. Code of conduct
5. Proactive monitoring
6. Complaints procedure
7. Enforcement
8. Relations with protagonists

We stress that it is not always easy to make a clear distinction between criteria. This is in particular so because some of them are interconnected. For this reason, some criteria should be evaluated or red in parallel.

Eventually, this “pragmatic list” of criteria was also used to identify a number of legal criteria a trustmark scheme should necessarily have. These so-called “**must-have**” criteria have been chosen because of their legal added value.

Although opinions may differ, this distinction can be advocated. Of course all legal obligations – for instance the Directive on electronic commerce – have to be respected. However, we advocate that for the evaluation of a trustmark scheme it is important to know to what extent the latter adds something extra to an e-platform or the existing obligations of positive (hard) law. Indeed, we underline that a criterion merely reflecting hard law provisions should not be retained as “**must-have**” because trustmark schemes’ subscribers – by law – must comply with them. In other words, they are *in se* “**must-have**” criteria.

In contrast to the remaining list of “*nice-to-have*” criteria, the list of fourteen “**must-have**” criteria allows to have a better general understanding of the legal quality of a trustmark scheme and their respective position in relation to the other schemes.

²³ See, *infra* section 4.3. Also see Benchmark criteria; WP 2: List of relevant criteria and regulations.

Each of the criteria, both “*must-have*” and “*nice-to-have*” shall be evaluated according to a two-phased procedure:

- § Phase 1: **vertical evaluation** of each trustmark scheme with comments on each criterion;
- § Phase 2: **horizontal evaluation** of the trustmark schemes assessed in the first phase. During this phase and as a result of the comments made, a value on a scale of five will be given to each criterion²⁴.

To avoid an ambiguous interpretation of the results, it is specified to what the following values correspond (scale of 5):

- § 5: very good, even excellent
- § 4: good
- § 3: average
- § 2: need to be improved
- § 1: non-existent to poor

For a more elaborated view on the legal assessment methodology, in particular for a comment on the different sources of law, reference is made to the annexed WP 2 regarding the methodology and comments of criteria. It is however, important to emphasize the following points:

- § The evaluation is an “**on sight desk evaluation**”²⁵: Only information that is publicly available on the trustmark scheme’s website is considered. To stimulate both consumers’ and businesses’ confidence, it is of paramount importance that the public receives comprehensive and transparent information on the scheme’s functioning and characteristics. For this reason it is important that consumers are allowed to verify the functioning of the concerned trustmark scheme. What they do not know, they cannot verify, nor can it stimulate their confidence. In other words, what happens in the scheme’s internal “black box” does not stimulate confidence.

Therefore, back office information that is made available on request, e.g., the over 300 pages code of conduct of *Webtrust Netherlands*, is excluded from the scope of evaluation.

- § The **evaluation focuses on the “second-level applications” of complex models** (hierarchical and hybrid trustmark scheme models). A variety of organisation models exists among the selected trustmark schemes. Besides classical *stand alone* models, a certain number of models are characterised by their structural complexity. While some complex trustmark schemes are based on a *hierarchical* structure²⁶, others have

²⁴ Whereas five reflects the maximum value.

²⁵ The evaluation takes into account the information published on the website of the Trustmark scheme on 1 November 2004. Information that is only made available upon request, is not considered in the present evaluation.

²⁶ In the sense that an organisation accredits trustmark schemes that comply with the “hierarchical” code.

a *network* structure²⁷. Eventually, some are *hybrid*, i.e., a combination of a hierarchy and a network structure²⁸.

The existence of complex models – especially those constituted by different levels (hierarchical or hybrid structures) – raised some methodological difficulties as to the choice of the structural level that would be the subject of the evaluation. To make a meaningful comparative evaluation, it was decided to focus on the concrete applications (lower or second level) of the complex models²⁹, so that all the trustmark schemes could be benchmarked on the same level. The principle reason to opt for this level is because it has the most direct impact towards subscribers and consumers.

In this context, *Labelsite* – the French application of the hierarchical organisation Euro-Label – and *SafeBuy* – one of the schemes accredited by TrustUK – were selected³⁰.

- § The **evaluation is made at a certain time** (time stamped). For this reason, one cannot guarantee that providers of ‘trusted services’ made modifications to their trustmark scheme. This is in particular so because it was noticed that during the short time lapse between the vertical evaluation and the horizontal one, some schemes had already been modified or further developed³¹. So one might not exclude that the (temporary) assertions remain 100% valid at the moment of the publication of the project’s findings. The fact that trusted websites are modified frequently pleads for the obligation of each trustmark scheme to time stamp each version and to archive the previous versions in order to prevent litigation on the version existing at the precise moment of the labelled transaction.

- § This benchmarking activity implies to a certain extent a **subjective aspect** regarding the selection of criteria³² and the proper evaluation of each criteria.

²⁷ Where a network is composed by (consumers) organisations, each using their (different) national code concerned.

²⁸ That is based on a network of certification bodies that co-operate under the hierarchy of a particular organisation.

²⁹ The higher or top level of scheme was therefore not benchmarked.

³⁰ Nevertheless, considering the high number of second level applications of the *Qweb* scheme (twenty-two certification bodies, including twelve in Italy), the evaluation was conducted from the higher level of this hybrid scheme instead of picking a certification body at random.

³¹ See, for instance, Luxembourg e-commerce certified that has developed two other types of seals.

³² As to the identification of criteria, one has to bear in mind that most of the attributes of a trustmark scheme can be considered as part of a complex network of relationships. Therefore, the same attribute can be viewed from various perspectives.

4.3 List of criteria according to the life cycle

From different sources of hard and soft law, a number of criteria were identified. These criteria can be regrouped according to the eight phases of the life cycle of a trustmark scheme.

The table below contains these criteria. For a comment of the criteria and the reference towards their respective origin, we refer to the annexed WP2. We note that the criteria on a red band are **must-have criteria**.

1. ELABORATION OF THE TRUSTMARK SCHEME	
1.1. Legitimacy of the scheme	
1.2. Code of conduct	
	1.2.1. Clearness
	1.2.2. Multilingualism
	1.2.3. Access
1.3. Security and privacy	
2. INFORMATION ON THE TRUSTMARK SCHEME	
2.1. Identification of the trustmark scheme provider	
2.2. General information on the trustmark scheme's functioning	
	2.2.1. Trustmark scheme properties
	2.2.1.1. Scope and objectives
	2.2.1.2. Management
	2.2.2. Assessment's procedure
	2.2.2.1. Type and subject of the procedure
	2.2.2.2. Identity, composition and role of the assessment body
	2.2.2.3. Costs
	2.2.3. Code of conduct
	2.2.3.1. Normative references
	2.2.3.2. Update
	2.2.4. Subscribers participating in the trustmark scheme
	2.2.5. Monitoring
	2.2.6. Complaints procedure
	2.2.7. Alternative dispute resolution
	2.2.8. Sanctions
	2.2.9. Liability

3. PARTICIPATION IN THE TRUSTMARK SCHEME	
3.1. Accessibility of the trustmark scheme	
3.1.1.	<i>Open character</i>
3.1.2. Affordability	
3.1.3. Convenience	
3.2. Procedure of assessment	
3.2.1. Fairness of the assessment	
3.2.1.1.	<i>Independence of the Body</i>
3.2.1.2.	<i>Competence of the assessors</i>
3.2.2. Effectiveness of the assessment	
3.2.2.1.	<i>Time-span</i>
3.2.2.2.	<i>Methods</i>
3.3. Mutual recognition	
4. CODE OF CONDUCT	
4.1. General principles	
4.1.1.	<i>Trustmark localization</i>
4.1.2.	<i>Transparency</i>
4.1.2.1.	<i>Clear information</i>
4.1.2.2.	<i>Language and global dimension</i>
4.1.3. Fairness and social responsibility	
4.1.4. Applicable law and competent jurisdiction	
4.2. Information on the merchant	
4.2.1.	<i>Identity of the merchant</i>
4.2.2.	<i>Merchant's commitments</i>
4.3. Information on the products and services	
4.3.1. Characteristics of the products or services	
4.3.1.1.	<i>Clear description of the products/services</i>
4.3.1.2.	<i>Availability of the products/services</i>
4.3.2. Prices	
4.3.3. Supply restrictions	
4.3.4. Delivery conditions	
4.3.5. Guarantees	
4.3.6. Duration of the contract	

4.4. Conclusion of the contract	
4.4.1. Contract terms and general conditions	
	4.4.1.1. Availability
	4.4.1.2. Means to store and reproduce
4.4.2. Order procedure	
	4.4.2.1. Clear information
	4.4.2.2. Confirmation process
	4.4.2.3. Placing the order (acknowledgement of receipt)
	4.4.2.4. Written confirmation
4.4.3. Order error protections	
	4.4.3.1. Clear information
	4.4.3.2. Means to identify and correct handling errors
4.4.4. Cancellation/Refund terms	
	4.4.4.1. Information on a right of withdrawal/refund modes
	4.4.4.2. Information on refund modes
4.4.5. Payment	
4.4.6. Inertia selling/unsolicited services	
4.4.7. Filing of the contract	
	4.4.7.1. Clear information
	4.4.7.2. Accessibility
4.5. Customerservice	
4.5.1. Information on the customer service & contact point	
4.5.2. Complaints procedure	
	4.5.2.1. Clear information
	4.5.2.2. Principles
4.5.3. Information on alternative dispute resolution	
4.7. Commercial communications and fair marketing practices	
4.7.1. Commercial communications	
4.7.2. Fair marketing practices	
4.7.3. Unsolicited communications	

4.8. Security of system and payment	
	4.8.1. Information & contact point
	4.8.2. Technical requirements
4.9. Personal data protection	
	4.9.1. Reference to privacy policy
	4.9.2. Information
	4.9.2.1. Identity of the controller
	4.9.2.2. Purpose of the process
	4.9.2.3. Recipients
	4.9.2.4. Right of access and rectification
	4.9.3. Notification to national DPA
4.10. Protection of children	
	4.10.1. Commercial communications and fair marketing practices
	4.10.2. Harmful content
	4.10.3. Data protection

5. PROACTIVE MONITORING	
5.1. Monitoring mechanisms	
	5.1.1. Fairness
	5.1.2. Effectiveness
5.2. Monitoring reports	

6. COMPLAINTS PROCEDURE	
6.1. Accessibility and convenience	
6.2. Quality of the complaints procedure	
	6.3.1. Fairness
	6.3.2. Effectiveness
6.3. Alternative dispute resolution	

7. ENFORCEMENT SYSTEM	
	7.1. Fairness
	7.2. Effectiveness
	<i>7.2.1. Sanctions towards subscribers</i>
	<i>7.2.2. Remedies for consumers</i>

8. RELATIONSHIPS WITH PROTAGONISTS	
	8.1. General relationships
	8.1.1. Feedback
	<i>8.1.2. Report on activities</i>
	<i>8.1.3. Additional services</i>
	8.2. Relationships with consumers
	<i>8.2.1. Validity of certification</i>
	<i>8.2.2. Privacy Policy</i>
	8.3. Relationships with business
	<i>8.3.1. Promotion</i>
	<i>8.3.2. Security & confidentiality</i>

4.4 Table of “*must-have*” criteria

The table below shows i) the value³³ given for each of the fourteen *must-have* criteria for each individual trustmark scheme, ii) the aggregated value for each criterion and iii) the total score of each trustmark scheme.

Table 4.4.1
Overview of *must-have* values

	Labelsite 	Safe Buy 	Qweb 	Webtrader 	Webtrust 	Trusted Shops 	e-Lux Certified 	Confianza 	Thuis winkel 	Criterion Score
1. Legitimacy of the scheme	2	5	1	3	1	5	5	3	4	64.44%
2. Access and clearness of the code of conduct	4	3	3	4.5	1	3.5	4	5	3	68.89%
3. Information on trustmark scheme's functioning	3.69	3.08	2.69	2.23	1.77	3.31	3.08	3.46	4	60.69%
4. Assessment	4.25	1.5	2.25	1.25	1.5	1.5	4	1.5	3	46.11%
5. Feedback	3	5	3	3	3	4	4	3	5	73.33%
6. Applicable law & competent jurisdiction	3	1	5	4	1	4	1	1	4	53.33%
7. Confirmation process	5	2	4	5	1	3	5	5	1	68.89%
8. E-platform security	3.5	5	5	2.25	1	3.5	4	4	4	71.11%
9. Customer service	3.25	3.5	4	4.5	1	2.5	3.25	3.5	3.25	63.89%
10. Protection of children	5	3.33	4.33	4.67	1	2.67	3.33	4	1	65.18%
11. Proactive Monitoring	3	1.67	2.33	2	1.33	2.33	3.33	1.33	1	40.71%
12. Complaints procedure for solving disputes	1	2.5	1.25	1.25	1	4	2.75	4.75	3.75	49.44%
13. Enforcement system	2	1.67	2.67	1.67	1	3	1	3	1.67	39.29%
14. Relationships with consumers	2	1.5	3	1.5	2	4.5	3.5	3.5	3	54.44%
TMS Score	63.84%	56.79%	62.17%	58.31%	26.57%	66.87%	67.49%	64.34%	59.53%	

³³ For the avoidance of any doubt, it is specified to what the following values correspond (scale of 5):
 5: very good, even excellent
 4: good
 3: average
 2: need to be improved
 1: non-existent to poor

4.5 Findings and trends

General observations

Based upon the evaluation of the nine trustmark schemes some general observations can be made.

A first trend one may observe is a very general one: there are as many differences as there are trustmark schemes.

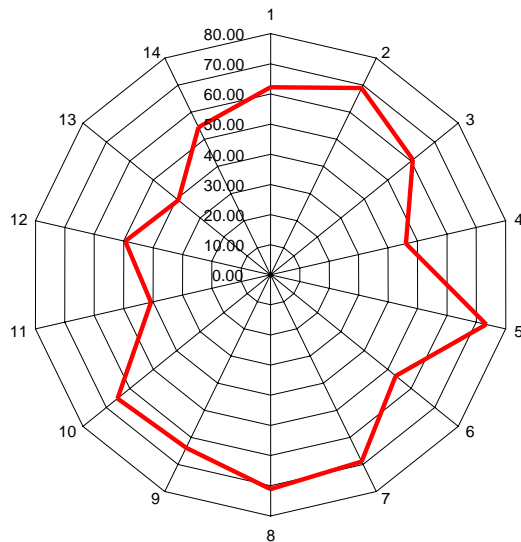
It seems that there is (almost) no (positive) correlation between criteria. Although on a micro level a positive evaluation for, e.g., legitimacy, may indicate transparency on the management structure of the scheme, this is not so on a macro level of the life cycle's phases or *must-have* criteria. *Vice versa*, the fact that a particular criterion is evaluated in a negative manner does not by definition imply that this is also the case for other criteria.

Indeed, based upon the present review of criteria, one has to conclude that some trustmark schemes have very good evaluation values for one, two or more phases (of the life cycle) or *must-have* criteria. However, of the nine trustmark schemes, there is not one that has positive values (three or more) for every *must-have* criteria. In this context and from a legal point of view, it is difficult to understand why certain trustmark schemes demonstrate their quality while elaborating and implementing good self-regulatory principles, but, e.g., fail to inform consumers in a transparent way or do not allow user-friendly registration methods for code of conducts and other rules. One explanation for this can be found in the fact that some trustmark schemes prefer to start with a small-scale model that grows to a full-scale trust model, this instead of kicking off with it.

This is clearly demonstrated in figure 4.5.1. The evaluation of the fourteen *must-have* criteria is not very consistent. Some criteria, e.g., elaboration of the Code of Conduct or protection of children, are evaluated in a positive manner, while other criteria seem to have a rather low score.

This trend is particularly valid for the monitoring and enforcement mechanisms. We underline that the three metacriteria, – i.e., criteria n° 11 (proactive monitoring), 12 (complaints procedure for solving disputes) and 13 (enforcement system) – have a negative average evaluation between 39% and 49%. In other words, the scheme can be as comprehensive and consumer friendly as one could wish, if its principles are not enforced, the quality and the long- term existence of the trustmark scheme can be questioned.

Figure 4.5.1
Overview of 14 *must-have* criteria



1. Legitimacy of the scheme
2. Access and clearness of the code
3. Information on TMS' functioning
4. Assessment
5. Feedback
6. Applicable law & competent jurisdiction
7. Confirmation process
8. E-platform security
9. Customer service
10. Protection of children
11. Proactive Monitoring
12. Complaints procedure for solving disputes
13. Enforcement system
14. Relations with consumers

A second trend is that most of the trustmark schemes are characterised by a lack of “European sensitivity”.

Even if the benchmarking reveals that all existing initiatives have their particularities and are different from each other, it can be noted that trustmark schemes lack of what one could call a “European sensitivity”.

In this respect, trustmark schemes should get more involved in the development of a more general confidence-building strategy at European level. This observation is derived from a number of elements emphasised by the benchmarking. This allows to make some recommendations:

- § The difficulties to face cultural differences and languages: only few trustmark schemes give sufficient attention to the problem of cultural and linguistic differences. At present, most of them do not offer an adequate bilingual or multilingual service.
- § The lack of articulation and co-ordination between the different trustmark schemes: it must be underlined that most of trustmark schemes seem to be restricted to their own territorial scope, without taking into account the global dimension of the internet and the inherent transnational character of the commercial transactions.

In this context, a trustmark scheme should consider developing mutual recognition or similar arrangements with trustmark programs in other countries or regions. In this way, merchants certified under a program that complies with these guidelines, can be identified by consumers in other jurisdictions as offering the same level of trust and protection.

- § The lack of reference to (and involvement in) the existing EU initiatives regarding e-confidence and consumer protection³⁴. In this respect, the most outstanding example is the lack of information given by trustmark schemes regarding the existence of the European Extra-Judicial Network for cross-border dispute resolution (EEJ-Net).

Therefore, one could require from trustmark schemes to provide transparent and adequate information about relevant EU initiatives. In an ideal system, trustmark schemes could also act as a kind of contact point or “clearing house”, in particular towards merchants, notably SMEs.

A third observation relates to the European Trustmark Requirements.

Considering the number of benchmarked trustmark schemes and the differences observed between them, it is difficult to have a general overview on their degree of compliance with the European Trustmark Requirements (ETR).

Nevertheless, due to the high level of standards included in the ETR, one could conclude that general or complex trustmark schemes could be more inspired by this normative instrument.

According to the nine (9) areas covered by the ETR³⁵, one has to formulate the following observations.

- § Even if trustmark schemes have a rather good evaluation of “transparency” (information published on their website), efforts can be made for the presentation of the information as required in the section 2 of the ETR. It means that information provided at any stage could notably be presented in easy accessible manner (user-friendly).

Moreover, accurate information should be provided on the identity and the role of the (independent third) body in charge of the assessment. Finally, trustmark schemes should also publish an annual report on their activities. The benchmarking revealed that this was not very often done.

- § For the content of the code of conduct, it must be underlined that in some areas the ETR are surprisingly more complete than some of the benchmarked codes. Therefore, trustmark schemes should pay a particular attention to a more careful and accurate drafting of the code which, unlike the ETR, directly applies to merchants.

Fore instance, in comparison with the ETR, codes of conduct could:

³⁴ See Special Eurobarometer European Commission, “Issues relating to business and consumer e-commerce”, Executive Summary, March 2004, p. 20: “*Only one in ten EU15 citizens had heard of Internet trust marks. Relatively high levels of awareness were observed in Austria (19%), Denmark (16%) and Germany (15%). At the other end of the scale, awareness of trust marks had only reached 6% of Italians and Portuguese and 7% of Greeks and Spaniards. Surprisingly, the Swedes – the country which throughout this survey has shown the highest awareness and usage of the Internet – had only 8% of its poll being aware of trust marks*”.

³⁵ The ETR address the following issues: 1. High standards, measurability and purpose of trustmark scheme; 2. Transparency of trustmark schemes of consumers and business; 3. Accessibility and visibility of trustmark schemes for consumers and business; 4. Scope and content of trustmark schemes (content of the code of conduct); 5. Operation of trustmark schemes; 6. Assessment of applicants for trustmark schemes; 7. Monitoring system; 8. Enforcement system; 9. Technical security.

- Include more constraining requirements as regards marketing practices³⁶;
 - Promote higher levels of customer service (which should be responsible, flexible, efficient and not only dedicated to consumer complaint handling)³⁷;
 - Impose high requirements regarding the accessibility and transparency of contract terms and general conditions;
 - Contribute to make the legal provisions concerning the order procedure more understandable to their subscribers;
 - Impose in a more systematic way guiding principles of a company's complaints handling and customer redress system. This way, it could help merchants to implement a transparent and fair redress system.
- § Concerning the assessment process, it must be underlined that the ETR could be more wordy and precise in such an important area. Nevertheless, the ETR recommend trustmark schemes to have a clear procedure in place for the assessment of applicants³⁸. The benchmarking reveals some important transparency deficiencies in this area. The websites sometimes do not even mention which body is in charge of this function, its role, the composition of the assessment body and, eventually, how the process is handled.
- § For the monitoring system, the benchmarking reveals that metatrustmark schemes meet the recommendations of the ETR³⁹. Trustmark schemes use the “mystery shopping” method to monitor their subscribers and encourage feedback from consumers and other interested parties. Nevertheless the regularity and the quality of the controls can substantially differ from one trustmark scheme to another.
- § Regarding the enforcement system and especially sanctions, most of the trustmark schemes do not really meet the ETR⁴⁰. The latter make explicit reference to the necessity to foresee a plurality of sanctions: “*a list of dissuasive and proportionate sanctions should be established*”. But most of trustmark schemes only focus on the withdrawal of the trustmark which is the most radical possible sanction, without apprehending this sanction as the ultimate step of a gradual coercion-scheme⁴¹.

Furthermore, the enforcement process is not always as transparent as recommended by the ETR. Trustmark schemes should provide more information on the body in charge of the procedure and the principles of the procedure itself. This remark is also valid for the publication of the enforcement decisions. The benchmarking demonstrates that in most cases trustmark schemes do not mention or foresee the publication of the sanctions undertaken against the merchants concerned.

Eventually, it must be emphasised that even if the ETR include high-level standards towards trustmark schemes, they do not directly address some important aspects of trustmark services. In this view, reference is for instance made to the confidentiality and protection of

³⁶ In our opinion, a code's provision simply stating that the subscribers have to comply with the national legislative framework or with other self-regulatory guidelines in this area cannot be considered as an adequate requirement!

³⁷ See section 1 of ETR.

³⁸ See section 6 of ETR.

³⁹ See section 7 of the ETR. The ETR should specify more precisely the different types of controls that can be undertaken to monitor the compliance of a subscriber with the code of conduct.

⁴⁰ See section 8 of ETR.

⁴¹ See, *infra*, phase 7 (enforcement).

(personal as well commercial) data gathered by a trustmark scheme. Or they do not sufficiently insist on complaints procedures and alternative dispute mechanisms.

4.5.1 Phase 1: Elaboration of the trustmark scheme

In this first phase of the life cycle, the specific characteristics of a trustmark scheme that play an important role to create credibility, trust and confidence *vis-à-vis* both consumers and businesses have been analysed.

Legitimacy

This criterion aims to evaluate whether the selected trustmark schemes are elaborated on a legitimate basis. For that purpose different factors were analysed.

First of all, particular attention was paid to the *involvement of all interested parties* (stakeholders) within the trustmark scheme. In this regard, we have focused on i) the participation of representative business organisations of the sector and ii) the degree of consumers' involvement.

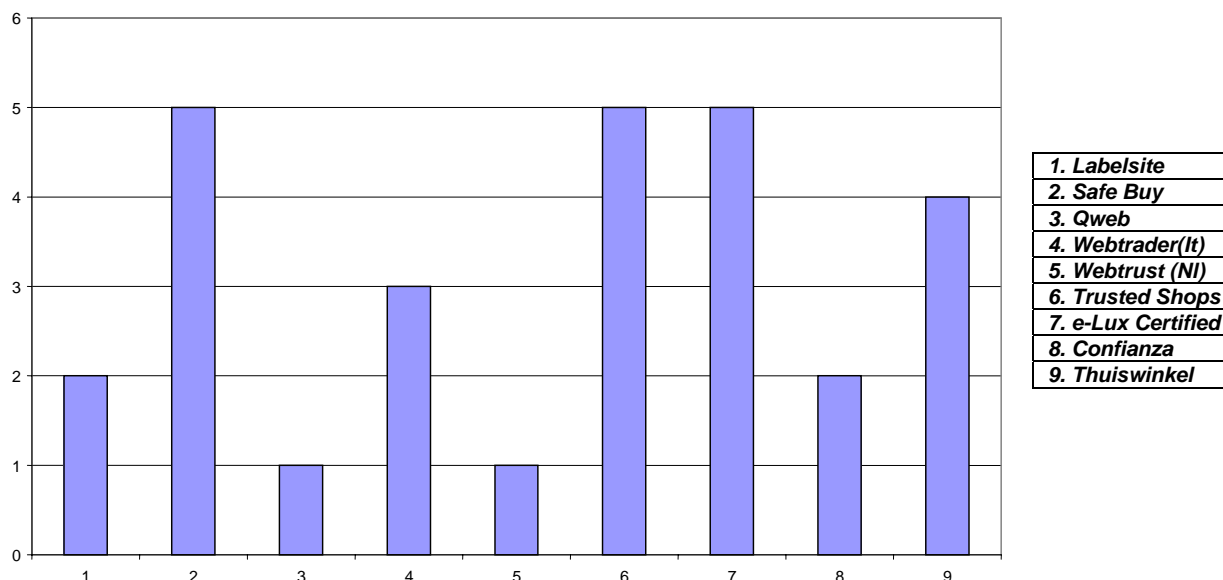
The benchmarking reveals different degrees of consumers' involvement: it can vary from a simple submission of the draft code to a consumers association (*a posteriori*), a co-participation in the elaboration of the scheme, especially in the drafting of the code of conduct, to an active intervention of consumers' representatives in the scheme.

This last aspect also refers to another important aspect of the legitimacy principle: the creation and the *intervention* in the overall functioning of a trustmark scheme of an "*independent*" council or board – composed on a (balanced) representation of all interested parties. This council can be important to ensure the objectivity of requirements for online shops as well as maintain an egalitarian approach⁴².

In general, one can observe that four of the nine analysed trustmark schemes do not favour the involvement of all interested parties: three were launched only by industry or professional organisations (Eurolabel/Labelsite, Qweb, Webtrust), one was launched only by consumers associations (Webtrader). Moreover, these trustmark schemes do not have an "independent" council or board. Labelsite has a "Comité d'habilitation", but this body is only composed by representatives of the professional sector.

⁴² See, for instance, the "Comité de certification" of Luxembourg e-commerce certified that can be considered as a reference model, <http://www.e-certification.lu/comite.htm> : "*Dans un souci de transparence, les propriétaires du certificat ont souhaité mettre en place un comité de certification regroupant des partenaires institutionnels, des représentants du secteur industriel et des consommateurs ainsi que des professionnels d'internet. Cette structure indépendante, regroupant des compétences multiples et des intérêts divers, apporte une vision et une expertise supplémentaire qui garantit le respect des règles déontologiques du processus de certification*".

Table 4.5.2.1
Legitimacy of the scheme



Finally, it was examined whether the trustmark initiative is supported or endorsed, directly or not⁴³, by a public authority, both at a national (national government) or an international level (European Commission). In this respect, one may conclude that some trustmark schemes are supported or endorsed by European authorities, some other by national public bodies. Other trustmark schemes do not have any public support whatsoever⁴⁴.

Table 4.5.2.2
Overview of public support/endorsement

Public support		No public support
EU	National government	
1. Labelsite (via Euro-Label) 2. Webtrader Italy 3. Trusted Shops	1. SafeBuy (via Trust UK) 2. Luxembourg e-commerce certified ⁴⁹	1. Webtrust NL ⁴⁵ 2. Qweb ⁴⁶ 3. Confianza Online ⁴⁷ 4. Thuiswinkel ⁴⁸

⁴³ By “indirect”, we mean that we have also taken into consideration the public support offered to overarching structures, also referred to as “metalabels”.

⁴⁴ The logo of the supporting authority is generally displayed on the trustmark scheme’s website.

⁴⁵ This trustmark scheme is supported by a specific professional body, Het Koninklijk Nederlands Instituut van Registeraccountants (NIVRA).

⁴⁶ This trustmark scheme is supported by a worldwide international certification network (IQNet).

⁴⁷ This trustmark scheme is supported by professional organisations as AECE (Asociación Española de Comercio Electrónico), AUTOCONTROL (Asociación para la Autorregulación de la Comunicación Comercial) and IAB Spain (the Interactive Advertising Bureau of Spain);

⁴⁸ This trustmark scheme is supported by professional organisations co-operating under the Nederlandse Thuiswinkel Organisatie (Thuiswinkel.org).

⁴⁹ Luxembourg e-commerce certified is supported by the Ministère de l’Economie et du Commerce extérieur.

As a general conclusion regarding the criterion of legitimacy one can make the following observations:

- § In the first place, one can conclude that globally the trustmark schemes are developed on a legitimate basis (64, 44%). This is in particular so in view of the participation of all interested parties. In this respect, one can observe that even if a trustmark scheme is not supported by a public authority, this circumstance does not necessarily imply that the initiative is unilateral. For instance, the code of conduct and the general conditions of *Thuiswinkel* - which is not as such supported by a public authority – have been submitted for examination to a well-known consumer association in Netherlands (Consumentenbond).
- § Secondly and more surprising, one can note that a support or endorsement by a public authority does not necessarily and automatically imply an irreproachable quality of the trustmark scheme itself. Even more, some codes of conduct do not even or not necessarily respect the applicable law. Therefore, the link between these two elements – the public support and the quality of the scheme – seems not to be so obvious. In this view, one can recommend that at European level some minimum sets of criteria are defined. Every time a public authority, in particular the European Commission, supports or endorses a self-regulatory initiative, these minimum standards have to be met and respected.

This observation can concern different aspects of a trustmark scheme. This is illustrated by the following examples.

- Regarding the enforcement, *Luxembourg e-commerce certified*, supported by the Ministère de l'Economie et du Commerce extérieur, does not provide any information on the sanctions that can be undertaken against subscribers.
- Regarding the complaints procedure, *Labelsite* does not provide any information on its website. This finding is as much surprising as Euro-label (the overarching structure), supported by the European Commission, which provides specific services (specific entry on the website and a complaint form) to assist consumers with complaints relating to the activities of Euro-Label certified shops. More serious is the fact that the website of *Labelsite* does not refer anywhere to the overarching metastructure it is derived from (no logo, no hyperlink)!
- For the content of the code of conduct, one could expect from initiatives supported by public authority that obligations imposed on subscribers are more complete or better formulated. This is not always the case. For instance, the code of conduct of *Trusted Shops* supported by the EU Commission could be more developed in important matters such as the protection of minors⁵⁰.

⁵⁰ The certification criteria (art. 3) refer to protection of children in one single paragraph: “*The online shop shall, by means of age verification mechanisms (e.g. copy of personal identity card/ identification card combined with an account number or credit card number registered under the same name), particularly undertake to ensure that goods whose sale is only permitted to adults are not supplied to minors and that contents which are morally harmful to adolescents are not accessible to minors*”.

Code of Conduct: Accessibility and clearness

According to the methodology, the accessibility and the clearness of the code of conduct have been considered a must-have criterion.

In this respect, some critical comments must be formulated.

- § The benchmarking reveals that in some cases the code of conduct is not conspicuously made available on the trustmark scheme's website⁵¹. Trustmark schemes should pay attention to this aspect because it is crucial, especially for merchants, that they are able to identify the source of their obligations; the code of conduct should therefore be posted directly on the homepage.
- § Regarding the terminology, trustmark schemes should privilege the use of understandable and common terms as they refer to the obligations imposed on subscribers (e.g., code of conduct, code of practice). The use of terms as *certification scheme, obligations, certification criteria, referential* should be avoided.

Moreover, some trustmark schemes use different terms to make reference to a same document. They should harmonise their terminology⁵².

- § One of the most important observations regarding the accessibility of the code of conduct – as functionally defined in the methodology (all the obligations imposed to the subscribers) – concerns the dissemination of subscribers' obligations in different normative sources. In several schemes those obligations are shared in two or three distinct documents as the code of conduct (certification criteria), the general terms and conditions of membership (contract between the scheme and the merchant), and, for instance, a specific document regarding the dispute-resolution process⁵³.

This circumstance is not a substantial problem. Nevertheless, it could lead to some confusion if the trustmark schemes do not conspicuously provide information on the existence of these sources, or even worse if the information is difficult to find⁵⁴.

- § Regarding the clearness of the code, trustmark schemes globally have good evaluation values. Nevertheless, some observations can be formulated.

An aspect that was - generally - not covered by codes concerns the meaning of technical terms and jargons used in the codes. In the e-commerce field, the meaning of words like *webtrader, service provider, trustmark, certifier*, etc. are not unequivocal

⁵¹ All the codes of conduct are available on the internet, except the one of *Webtrust NL*.

⁵² This observation also concerns the "privacy policy". *Trusted Shops*, for instance, uses different terms on its website to refer to the same text: privacy, privacy policy, data protection policy.

⁵³ See for instance the homepage of *Thuiswinkel.org* (entry "Thuiswinkel Waarborg"), <http://www.thuiswinkel.org/index2.asp>. Clear reference is made to three documents: *Gedragregels* (code of conduct), *Algemene Voorwaarden* (general conditions) and *Reglement Geschillencommissie* (complaint rules).

⁵⁴ See notably the English version of the *Trusted Shops'* website, where one has to look hard for the "General Terms and Conditions of Membership". These terms can be accessed via a hyperlink placed at the bottom of the application form. In the French version of the website, this important piece of information does not seem to be available.

and often vary between languages. Trustmark schemes should more often foresee a specific section in their codes dedicated to terms, definitions and abbreviations⁵⁵.

A more general remark on the drafting method is that trustmark schemes should not hesitate to multiply the subtitles and paragraphs to increase the understanding of their codes of conduct.

Code of Conduct: Multilingualism

The multilingual character of the code can serve to evaluate an aspect of what one could call the “European sensitivity” of a trustmark scheme. The benchmarking surprisingly reveals that only three trustmark schemes (of the nine analysed) make their code available in different languages⁵⁶.

Moreover, it can be observed that there is no automatic correlation between the multilingualism of the code and the multilingualism of the trustmark scheme’s website, or the opposite. For instance, the content of *Webtrader Italy*’s website is only edited in Italian while two versions of the code are available (Italian and English). In contrast, the content of *Confianza Online*’s website is edited in two languages (Spanish and English), while only a Spanish version of the code is available.

Nevertheless, it must be underlined that in most cases the unilingualism of the code seems to reflect the geographical scope of the trustmark scheme. It means that the code is made available in the language of the potential webshop customers.

In this context, one could expect a greater coherence from trustmark schemes when they opt for a multilingual approach. In addition, one has to consider that the deficiencies observed in this area (language of the code and the website) are valuable indicators of the state of the art regarding the actual usefulness and capability of trustmark schemes to face the challenge of (confidence in) transborder e-commerce at European level.

Table 4.5.2.3
Comparison of languages

Trustmark schemes	Code of conduct	Website
1. Labelsite	French	French
2. SafeBuy	English	English
3. Qweb	English	English - Italian
4. Webtrader Italy	Italian - English	Italian
5. Webtrust NL	not available on internet	Dutch
6. Trusted Shops	German – English - French	German – English - French
7. Lux. E-commerce certified	French - English	French
8. Confianza Online	Spanish	Spanish - English
9. Thuiswinkel	Dutch	Dutch

⁵⁵ This aspect has also been observed by G. NANNARIELLO, *E-commerce and Consumer Protection – A survey of codes of practices and certification processes*, Joint Research Center, Institute for the Protection and security of the Citizen Cybersecurity sector, 2001, p. 35.

⁵⁶ Moreover, some differences, sometimes important, regarding the structure and/or the content of the code have been observed among the different linguistic versions of a code.

Security and privacy

Regarding security and privacy issues, the benchmarking reveals that most trustmark schemes do not provide sufficient information or any information on their practices⁵⁷.

This circumstance is particularly disturbing because trustmark schemes gather and process data necessary for the providing of their services. For instance, , both personal and commercial data, the most obvious case of data processing, are gathered when potential subscribers fill out an application form to participate in the scheme. Personal data can also be collected, especially from consumers, for dispute-resolution purposes.

A statement as found at the bottom of the *Luxembourg e-commerce's* form⁵⁸, is an outstanding example of the efforts that have to be made by trustmark schemes in this area.

In this context, trustmark schemes should be aware that they can be considered “data controllers” in the meaning of Directive 95/46/EC⁵⁹.

Therefore, they should systematically give information, for instance, in the form of security or privacy policies. A visible hyperlink not only on the homepage, but on every page, should bring the visitor to a page containing the relevant policy. Such policy should provide information on:

- § The security mechanisms used to protect the integrity and confidentiality of the data;
- § The data processing and its consequences:
 - The identity of the data controller;
 - The purposes of the processing for which the data are intended;
 - The recipients or categories of recipients of the data (if appropriate);
 - The existence of the right of access to and rectify the data, etc.

4.5.2 Phase 2: Information on the trustmark scheme's functioning

In this section, the information provided by the trustmark scheme on its functioning was analysed. Considering the large number of microcriteria composing this section, we will therefore limit our comment to some general, but crucial, observations. For the specific results, we refer to the comparative table in the annexed WP 2.

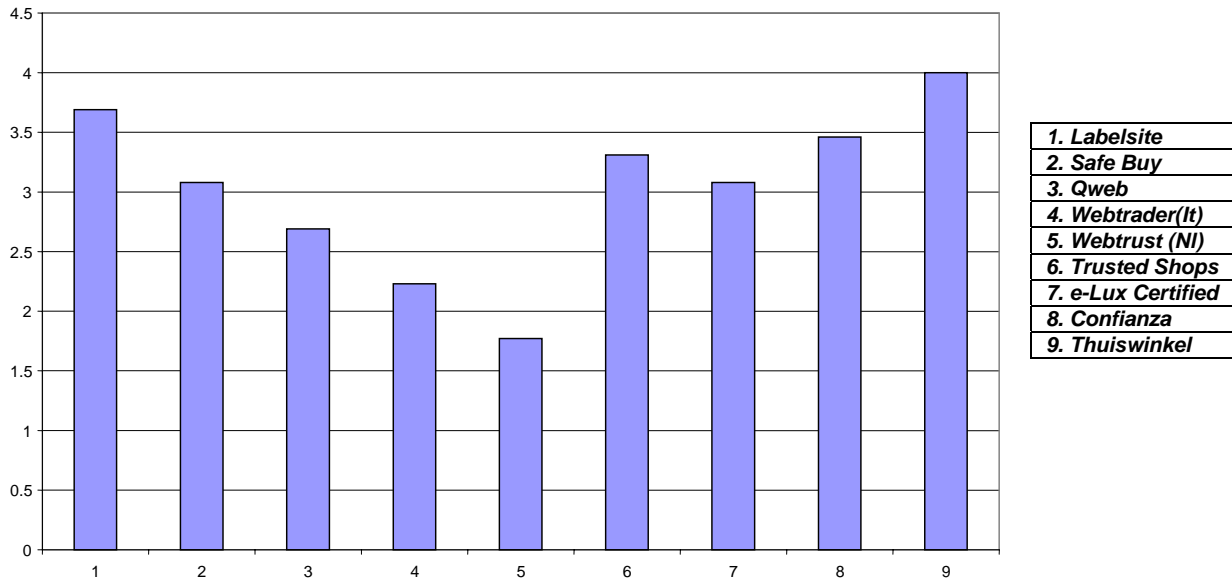
⁵⁷ This observation must be put in parallel with the results concerning phase 8 dedicated to the “relationships with protagonists”.

⁵⁸ See *Luxembourg e-commerce's* website (entry “Entrée en relation”), <http://www.e-certification.lu/srelations.htm>.

“*Ces données seront traitées avec discrétion absolue, et ne seront en aucun cas transmises à un tiers*”

⁵⁹ See article 2 (d) of the Directive: The “data controller” is 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; (...)”.

Table 4.5.3.1⁶⁰
Information on TMS functioning



General comments

- § From a general point of view, the benchmarking demonstrates that trustmark schemes provide transparent information on their functioning (60, 69 %). Nevertheless, some of them are failing to provide adequate and/or accurate details in some crucial areas such as management structure, identity and role of the assessment body, monitoring and complaints procedure or sanctions.
- § In order to improve the credibility of the information provided on their websites, trustmark schemes should ensure they provide clear information that is easy for visitors to find. In this regard, we recommend for instance inserting a direct link, direct web entry or that the information is clearly posted on the homepage. In particular, on a good site, most of this information should be easy to access from the homepage, so it will not take long to establish whether the site - or the provided service - is likely to be worth using.

The key disclosures should be located where a visitor (business or consumer) with no prior knowledge of the website could reasonably or intuitively expect to find them. A range of locations might be suitable for locating key disclosures, depending on what is being searched for (“About us”, “Certification”, “Code of conduct”, “Complaint”, ...). FAQs also count as easy to find, provided the information being sought is easily found by clicking on FAQs.

Furthermore, trustmark schemes should not hesitate to make conspicuous mention of the fact that more detailed information on one point or another is available in the code

⁶⁰ For the avoidance of any doubt, it must be stressed that the nine (9) numbers on the horizontal axe, refer to the benchmarked trustmark schemes: 1. Labelsite; 2. SafeBuy; 3. Qweb; 4. Webtrader Italy; 5. Webtrust Netherlands; 6. Trusted Shops; 7. Luxembourg e-commerce certified; 8. Confianza Online; 9. Thuiswinkel.

of conduct. For instance, *SafeBuy* refers to mediation in its code and encourages interested parties to read the relevant provisions: “*In the case of mediation, please read clauses 5.5 and 5.6 of the Code of Practice before contacting us*”⁶¹. Trustmark schemes should more regularly turn to this easy and inexpensive method of cross-referencing to information and information sources.

This observation pleads for the utilization by trustmark schemes of what one could call a “double language” system. Indeed, a trustmark scheme could develop and maintain in parallel two information systems; one formal and one informal. While in the first information system, the principles of the trustmark scheme are drafted from a stricter legal point of view, the second information system could rephrase the same information in a more user friendly, more understandable manner. For the latter purpose one could think for instance about a web section “FAQs”. Via internal hypertext links, both systems could be interconnected, synchronized and kept up to date.

- § We would like to underline the advantage for trustmark schemes to use modern technologies and internet to better edit and present information. In order to allow a fluent and coherent navigation - and to avoid a confusing dispersion of the information - trustmark schemes should increase the use of internal hyperlinks to establish easy links between the information contained in their website (cross-reference).

Showing a “human” face

- § The benchmarking reveals that some trustmark schemes (websites) have a very dehumanized or “impersonal” character. In our opinion, that could have some important consequences for the confidence one might have. This impersonal nature is mostly characterized by a lack of information regarding the management’s team and structure and more particularly regarding the individuals that “hide” behind the company’s name.

In this respect, the example of *Qweb*’s website is particularly relevant. In an entry “About us”, the visitors have to be satisfied with some very general, almost laconic, information on the fact that *Qweb* is “*offered by IQNet partners to IQNet customers as a new International scheme to satisfy the needs and the requirements of their operations in the net economy and to grant their customers the assurance of a compliant high quality on-line service*”... No further information is given.⁶² Almost the same remark applies to *SafeBuy*.

- § We believe, therefore, that adequate information regarding the management’s team and structure could without any doubt increase confidence. Furthermore, it is likely that people then feel more comfortable to deal with a trustmark scheme. Besides the strict compliance with hard law (the obligation of identification of article 5 e-commerce directive), the trustmark schemes should develop communication strategies towards consumers and businesses. In this respect, an interesting illustration of such a personal approach is the *Thuiswinkel*’s contact point. The website contains a specific

⁶¹ <http://www.safebuy.org.uk/contactus.htm>.

⁶² Moreover, the impersonal character of a trustmark scheme can be intensified by the formal structure of the website

entry (“Contact Opnemen”) where one can find photographs of the trustmark-scheme staff, with their contact address and relevant hyperlinks.

Relationship between trustmark schemes and metalabels

- § The benchmarking reveals some disparities between the trustmark scheme and the overarching hierarchical structure they derive from. More explicit information should be given regarding the participation of the trustmark scheme into such metasystem. For instance, *Labelsite* does not provide any information nor displays any logo related to *Euro-Label*.
- § Moreover, overarching top-institutions (metallabels) should impose a minimum harmonization regarding the website architecture (that has a clear influence on the quality of information) of the participating second-level trustmark schemes. Sometimes, the way sites provide information can vary greatly in the same hierarchical system. For instance, in the Euro-label model, a comparison between the French scheme (*Labelsite*) and the Austrian scheme (*Österreichisches E-commerce Gütezeichen*)⁶³ offers an interesting illustration of this lack of uniformity. The information should be presented in a standard format, not tailored to individual needs.
- § Eventually, we should also consider the potential advantages of such a two-level trustmark scheme structure. While we noted that some trustmark schemes can improve their manner of monitoring, by complying with the voluntary system, the metalabel could complement the enforcement mechanisms of the decentralized trustmark scheme. In connection hereto we also note that metalabels could have an important role in the settlement of cross-border disputes. If a German consumer, e.g., has a problem with a Dutch merchant, member of (a pan-European) metalabel, the German trustmark member could serve as complaint entry and complaint partner for the consumer, while the Dutch merchant is subject to the supervision of its national Dutch trustmark scheme.

4.5.3 Phase 3: Participation in the trustmark scheme

Open character & mutual recognition

Regarding the criterion “**open character**”, we have observed that even if most of the trustmark schemes provide adequate information on the scope and the objectives of their service, they do – mostly - not indicate the territorial framework of it.

For this reason, we must first recognize the practical limits of such a criterion and secondly be cautious about the relevance of the attributed scores. Nevertheless, too general information or a lack of information on this point may lead to the conclusion that the certification processes are mostly only open to merchants established in the country of origin of the trustmark scheme.

In some rare cases, however, trustmark schemes state that subscription will, in principle, be open to any interested organisation or person, regardless of their place of establishment⁶⁴.

⁶³ <http://www.guetezeichen.at/index.html>.

⁶⁴ See article 3 of the European Trustmark Requirements (ETR).

-
- § *Labelsité* states that : “Pour être habilité L@belsite, les sites intéressés doivent vendre en ligne des produits ou des services, en France ou à l’international, à des particuliers, à des entreprises ou des intermédiaires (...). Les sites peuvent être étrangers, à condition qu’ils aient une activité de vente en France (...)”⁶⁵.
 - § *Trusted Shops* states that : “The Trusted Shops certificate represents Europe’s number one sign of quality, allowing consumers throughout Europe to shop safely backed by the money-back guarantee – not to mention a whole range of other services and warranties”⁶⁶.

These observations raise the question of the development of **mutual recognition** between trustmark schemes and, more general, the question of the collaboration with other e-confidence programs.

In this respect, we have observed that some trustmark schemes mention the existence of other trustmark programs or the possibility to develop mutual recognition or similar arrangements. The following examples obviously illustrate that trustmark schemes do not consider this kind of initiative a priority:

- § *Labelsité* makes a brief reference to the principle of mutual recognition among the listing of the different competences of its “Comité d’habilitation”: *Décision de reconnaissance mutuelle d’autres sceaux*⁶⁷.
- § *Trusted Shops* only states: “We meet the requirements of consumer protection agencies as well as the recommendations of the TrustUK initiative.”
- § *Confianza Online* underlines the importance of such initiatives in its code of conduct: “De igual forma, considerando la globalidad y extraterritorialidad implícita de la world wide web y de los nuevos medios electrónicos e interactivos, este Código y los mecanismos de autocontrol establecidos para su aplicación tienen vocación de integración y/o coordinación en futuros sistemas internacionales de autorregulación para Internet y los servicios de la sociedad de la información, cuando sean una realidad”.

The assessment procedure

Considering the methodology used for the benchmarking, one has to bear in mind that the results related to the quality of the assessment procedure depends mainly on the information available.

In this respect, we may observe that metatrustmark schemes lack transparency. *SafeBuy*, for instance, merely states that “*SafeBuy vets all sites prior to accreditation ...*” and gives some

⁶⁵ See entry “L@belsite – Quels sites peuvent bénéficier du système L@belsite ?”

⁶⁶ See entry “Online shops – Your benefits”.

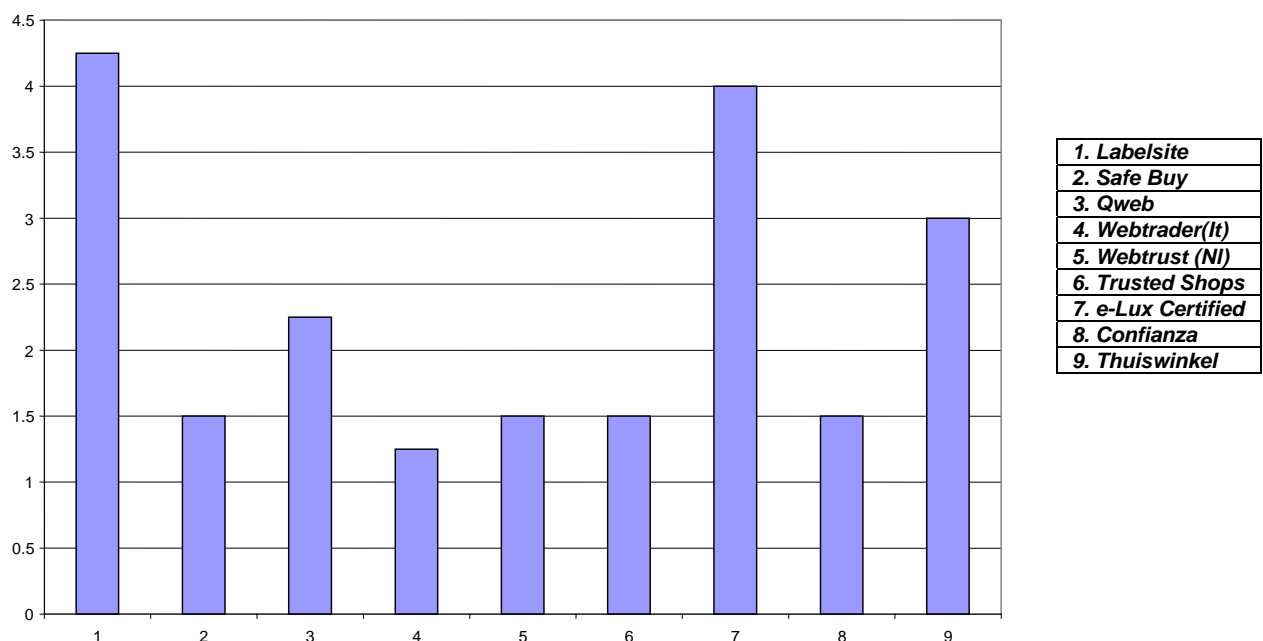
⁶⁷ See also the FAQs of *Euro-label*, n° 12 : “Can I also apply for and display seals or trust marks from other companies such as Verisign and TrustE (in addition to the Euro-Label Seal)? There is no restriction on the seals you may apply for and display on your site. The two companies named have seals that relate respectively to security and to privacy, neither of which offers the same qualifications as the Euro-Label mark”.

further information in its code of conduct. To receive further information on participation, *Trusted Shops* invites the potential applicants to request the “Information for Online Shops”⁶⁸.

According to the importance of the assessment in the overall functioning of a trustmark scheme, trustmark schemes should pay particular attention to information regarding the procedure of assessment and more particularly regarding the identity, the composition and the role of the assessment body.

One can note that more than half of the benchmarked trustmark schemes provide incomplete or unclear information on this point. However, in our opinion, this information is of crucial importance to allow potential applicants and interested consumers to evaluate the quality of the assessment, and thus, the credibility of the granted trustmark.

Table 4.5.4.1
Overview of Assessment procedures



Despite the lack of transparency mentioned above, it is however possible to draw certain general conclusions regarding the quality of the assessment procedure itself.

From the analysis of these processes, it appears that certification models which have a clear separation between the respective roles of the assessment body and the trustmark scheme (code owner) are much more reliable than others. That is to say that those schemes of certification, with a single code owner and one or more certifiers, holders of the know-how necessary to verify the standards, offer more reliability in terms of rigour and transparency.

The assessment procedure, for instance, proposed by *Luxembourg e-commerce certified* can be considered a model, notably because of the intervention of a “true” independent third body for the certification. The information given on this trustmark scheme’s website is as follows:

⁶⁸ See entry “Online Shops/Certification”. Nevertheless, *Trusted Shops* gives further information in its “General Terms and Conditions of Membership” which are particularly difficult to find.

“Elle (the certification) constitue une démarche volontaire de la part du prestataire de e-commerce qui souhaite obtenir le certificat. Elle est mise en œuvre à partir du moment où celui-ci dépose une demande de certification auprès d’un organisme certificateur accrédité (formulaire n° 001 – demande d’obtention, d’extension ou de renouvellement de la certification « Luxembourg e-Commerce Certified »).

Elle se base sur l’audit des exigences relatives à l’activité commerciale du prestataire (Le référentiel du certificat qualité « Luxembourg e-Commerce Certified ») ainsi que sur l’audit des aspects liés à la sécurité des transactions en ligne et à la confidentialité des données nominatives et personnelles (Le mini-guide de Sécurité des Systèmes d’Information). Ces deux audits sont menés en parallèle et la validation de chacun d’eux conditionne l’attribution du certificat qualité.

La demande de procédure de certification est dans un premier temps visée par l’organisme certificateur afin d’en mesurer la recevabilité par rapport aux spécificités du référentiel.

Une fois sa recevabilité constatée, l’organisme certificateur confie l’audit d’admission du prestataire de e-commerce à un auditeur.

Suite à cette évaluation, l’auditeur transmet au comité de certification (document n°003 : Règlement de fonctionnement du comité de certification) un rapport dans lequel sont notifiées les non-conformités relevées par rapport au référentiel ainsi que les actions correctives proposées par le prestataire’.

We may observe almost the same procedure for *Labelsite*. Concerning the other trustmark schemes, it seems (regarding the provided information) that there is a merger of different competences in one single body. Even if this procedure is carried out by competent assessors, questions on the independent and fair character of the procedure may arise. In many cases, those assessors are members of the trustmark scheme itself. In some cases, the trustmark scheme is directly provided by specialized certification bodies⁶⁹.

4.5.4 Phase 4: Code of Conduct

A. General comments

On the one hand, the benchmarking provides an examination about the content of the code of conduct and its compliance with the law (principle of legality). The code of conduct imposed by the trustmark schemes on its subscribers must indeed, in any case, be fully compliant with EU regulations. In this regard, trustmark schemes must comply with relevant EU legislation in relation to any obligation they place on subscribers or any practice they recommend to them. They should also require that subscribers take the necessary steps to ensure compliance with their legal obligations. Codes of conduct may not seek to override or replace any mandatory provisions at European level, and thus, they may not affect consumers’ statutory rights.

On the other hand, the benchmarking serves to determine the quality level of standards developed in each code of conduct associated with a trustmark scheme. More particularly, in addition to the principle of legality, codes of conduct are deemed to bring added value. In our opinion, the added value provided by codes can be twofold:

⁶⁹ See for instance the certification bodies of Qweb’s scheme (members of IQnet), the accountants of Webtrust Netherlands’ scheme (NIVRA), the assessors of SafeBuy’s scheme (Software Research Ltd.).

-
- § Codes can be used to demonstrate in greater detail how legislative requirements should be applied (*i.e.* explain complex concepts in ways that both consumers and merchants can understand)⁷⁰;
 - § Codes can be used to define norms or standards of behaviour for traders in areas where there are no specific legal requirements. On a methodological point of view, this specific aspect mainly deals with what we call the *must-have* criteria. Those criteria concern areas which are not directly addressed by legal provisions. They will be discussed in the last section of this chapter.

B. The general criteria related to the content of the code of conduct

In this section, we will address the criteria related to the content of the code of conduct that should be considered as *nice-to-have* in the sense that they all derive from legal sources.

Considering the large number of microcriteria composing this section, we will therefore limit our comment to some global but crucial observations. For the specific results, we refer to the comparative table in the annex (WP2).

Compliance with law

a) General comments

Regarding the legal aspect of a code, the benchmarking surprisingly reveals two types of deficiencies:

- § On the one hand, some codes fail to address important issues covered by EU legislation. For instance, *Webtrader Italy's* code of conduct does not include any requirement regarding (unsolicited) commercial communications. Even though this cannot be strictly considered an infringement of the law, it questions the value of codes of conduct.
- § On the other hand, some codes do not fully comply with EU legislation, in important areas such as the collection of personal data, unsolicited e-mails, and the order procedure.

In some cases, these 'deficiencies' can be explained by the difficulty to transpose in a comprehensive way the entire range of legal provisions applying to e-commerce activities into a few pages of a code of conduct. Furthermore, we note the sometimes difficult articulation between EU instruments as, *e.g.*, the distance selling Directive and the e-commerce Directive. In other cases, they seem to be caused by less excusable reasons of commercial opportunity, notably in the field of the collection of personal data for direct-marketing purposes.

⁷⁰ *Infra*, on *nice-to-have* criteria

b) Some examples

§ The quality of information

The benchmark reveals that most of the codes provide for adequate requirements regarding the information that has to be given by a merchant (accuracy of information). But, unfortunately, some codes do not require or do not sufficiently insist on the quality of this information. They should all require – either in the form of a general principle or by repetitive mentioning in the code – that this information should be presented in a clear and comprehensible manner, as required by the distance selling Directive (article 4) and the e-commerce Directive (articles 5 and 10)⁷¹.

For instance, the *Luxembourg e-commerce certified's* code only states that the merchant must give information concerning its identification of the products and services offered, without any stipulation on the clearness of this information⁷².

§ The conclusion of the contract (order procedure)

Regarding the order procedure, the benchmarking reveals that some codes of conduct do not always provide for adequate or transparent requirements. One reason could be the difficult and complex articulation between EU instruments as the distance selling Directive (hereafter DS-D) and the e-commerce Directive (hereafter EC-D).

To have a good understanding of the legal requirements for the B2C order process, both instruments must be read in parallel⁷³. Among others, the following provisions must be articulated: information on different stages to follow to conclude the contract and the technical means for identifying and correcting input errors⁷⁴ prior to the placing of the order (art. 10 EC-D), acknowledgement of receipt (article 11 EC-D), written confirmation on a durable medium (article 5 DS-D), etc. Moreover, from a practical point of view, certain provisions can be merged in one single requirement. For instance, a merchant could send to his customers a summary of the order in a durable medium (written confirmation) that is included when acknowledging receipt of the order (acknowledgement of receipt).

In this area, trustmark schemes should consequently be more careful in the drafting of their respective code, so that they do not mislead their subscribers by recommending them incorrect or ambiguous practices.

⁷¹ See, for instance, art. 5, § 1, e-commerce Directive: “*In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: (...)*”.

⁷² See, for instance, requirements n° 1 and 2 of the code
http://www.e-certification.lu/dpubli/livret001_e.pdf.

⁷³ E. MONTERO (sous la dir. de), *Le commerce électronique européen sur les rails. Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Cahiers du CRID, n° 19, Bruxelles, Bruylant, 2001.

⁷⁴ See the difference with the “confirmation process”, *infra*, p.

§ Direct-marketing practices

For direct-marketing practices, some codes of conduct show serious deficiencies. They either do not provide for any requirements in this area⁷⁵ or they are not fully compliant with EU regulations⁷⁶. More generally, it has been observed that some codes do not have adequately integrated the recent legal transition to the opt-in system⁷⁷.

Even worse, some codes even make recommendations that can be considered misleading practices. For instance, *Thuiswinkel's* code of conduct encourages its subscribers to pre-tick the opt-in box regarding the collection of the consumer's e-mail address⁷⁸. This of course blurs the distinction between opt-in and opt-out.

The added value

It would be wrong to assert that in all cases codes of conduct give added value to the existing EU provisions. The benchmarking shows that there are as many differences as there are codes. Moreover, sometimes codes impose high requirements in a particular area while in other areas they simply limit themselves by reproducing EU provisions.

Trusted Shops' code of conduct gives an outstanding example of this observation. While the code can be considered succinct regarding commercial communications, it imposes high requirements regarding the accessibility and transparency of contract terms and general conditions:

“In the event that General Terms and Conditions of Business should apply, they must be noted and clearly indicated (e.g. General Terms and Conditions of Business) on the online shop's entry page and in the immediate vicinity of the order button. The scope, structure, colours and font size shall be selected in such a fashion that perceptibility and comprehensibility are ensured at all times. General Terms and Conditions of Business must be formulated clearly and comprehensively in the mother tongue of the customers whom the range of products in question targets and it must be possible for such customers to save and reproduce such terms and conditions without difficulty”.

The benchmarking also reveals that codes generally give added value to the existing EU provisions regarding the cancellation and refund modalities by stating precise requirements and clearly distinguishing different hypotheses. It would be welcomed if this could be done by each trustmark scheme.

Finally, the benchmarking shows that added value can also be found by giving explanations, making comments on the code's requirements and by making recommendations that can be

⁷⁵ *Webtrader Italy's* code of conduct does not include any requirement regarding (unsolicited) commercial communications.

⁷⁶ *Thuiswinkel's* code of conduct (article 7 Privacy) seems to promote an opt-out system: “§ 2. Indien de consument aan het bedrijf te kennen heeft gegeven geen commerciële communicatie per post, telefoon, e-mail en dergelijke te willen ontvangen, dient deze wens gerespecteerd te worden”.

⁷⁷ See article 13 of the Directive 2002/58/EC on privacy and electronic communications.

⁷⁸ See *Thuiswinkel's* code of conduct (article 7, § 3): “Het bedrijf is verplicht op het ogenblik dat een consument zijn e-mailadres achterlaat op zijn website, hem te informeren over wat daarmee gebeurt. Daarmee heeft de consument de mogelijkheid aan te geven of hij al dan niet commerciële e-mails wenst te ontvangen. Dit gebeurt door een even grote JA- respectievelijk NEE-box op de relevante webpagina te presenteren. De JA-box mag vooraf aangevinkt zijn; de consument bepaalt met het (ver)plaatsen van het vinkje of hij wel of geen commerciële e-mails wil ontvangen. Tevens dient het bedrijf voor het verstrekken van e-mail adressen aan derden dezelfde mogelijkheden aan de consument te bieden”.

used by subscribers. This type of practice is useful to show in greater detail how to apply legislative requirements. Unfortunately, only one code of conduct makes such comments or recommendations systematically.

Labelsite's code of conduct, for instance, requires merchants to inform their customers about the implemented security procedures and makes specific recommendations for that purpose⁷⁹. *Labelsite* also dedicates an entire annex to the providing of specific recommendations on the protection of personal data.

C. The *must-have* criteria related to the content of the code of conduct

In this section, we will examine the criteria related to the content of the code of conduct that according to the methodology are considered *must-have* criteria because they go further than provisions of hard law. These criteria are:

- § applicable law and competent jurisdiction
- § confirmation process
- § e-platform security
- § customer service
- § protection of children

Applicable law and competent jurisdiction

As revealed by the benchmarking, few codes of conduct require merchants to inform their customers on the law applicable to the contract and the competent jurisdiction (53, 33 %).

Moreover, when such an obligation is included in a code, it is inaccurate or incomplete. For instance, in some cases, codes only focus on the applicable law without any reference to the competent jurisdiction.

The growing development of e-commerce, and especially the use of the Internet as a transnational and instant medium for business transactions, has resulted in a range of new laws and regulations. One of the major questions to be solved regarding e-commerce is the problem of which legal rules are applicable to cross-border consumer transactions by electronic means, both with regards to the law applicable to a B2C contract and to jurisdiction.

In general, cross-border contracts raise the following questions:

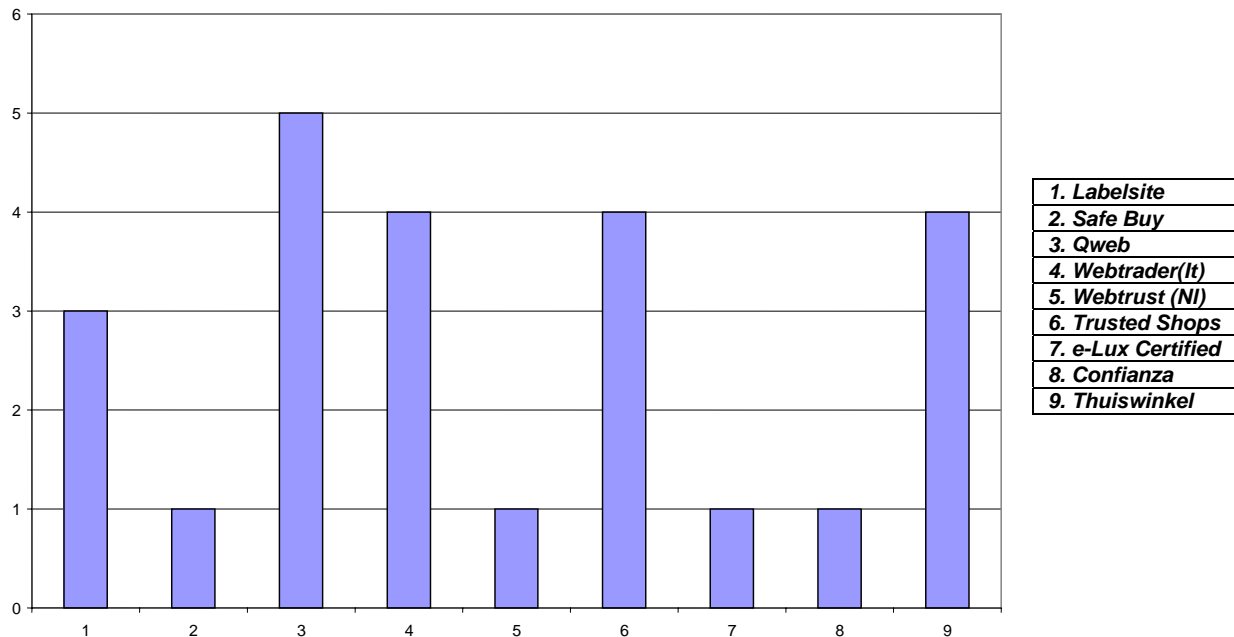
- § Which court is competent?
- § Which law is applicable to the contract?
- § How can a judgment be enforced?

The answers to these questions are provided by conflict of law rules of private international law, such as contained in the Brussels Regulation and the Rome Convention. For contracts concluded with a consumer, both instruments stipulate a special regime to protect the weaker party to the contract, *i.e.*, the consumer, by restricting the freedom of choice. A consumer, under certain circumstances cannot be deprived of the protection of the rules of

⁷⁹ See règle n° 10 : « Recommandation : *mettre, dans les pages d'information sur la politique vis-à-vis du traitement des données à caractère personnel, une phrase du type : "Conformément à la Loi Informatique et Libertés du 6 janvier 1978, les données personnelles que vous nous communiquez sont traitées et stockées dans des conditions visant à assurer la sécurité des informations" ».*

his home country. Consequently, if a consumer agreed on a choice of a law, which is not the law of his home country, he can invoke his home country regime in case of a dispute.

Table 4.5.4.1
Overview for Applicable law



Those questions are thus of major concern for consumers. For this reason, codes of conduct imposed on merchants in the framework of a trustmark scheme should as a key principle contain an obligation of transparency in this important area. *Trusted Shops*' scheme, for instance, seems to be fully aware of this important issue. Its code addresses the issue of applicable law in a clear and conspicuous provision and reminds the merchants of the withdrawal period rules according to the different EU members' national legislation⁸⁰.

Confirmation process

This criterion deals with the online contracting process. More particularly, codes of conduct should require merchants to provide consumers with an opportunity to review the transaction and to confirm their intent to enter into the transaction. In addition, they should indicate to consumers at what point a transaction will be final and becomes a binding obligation.

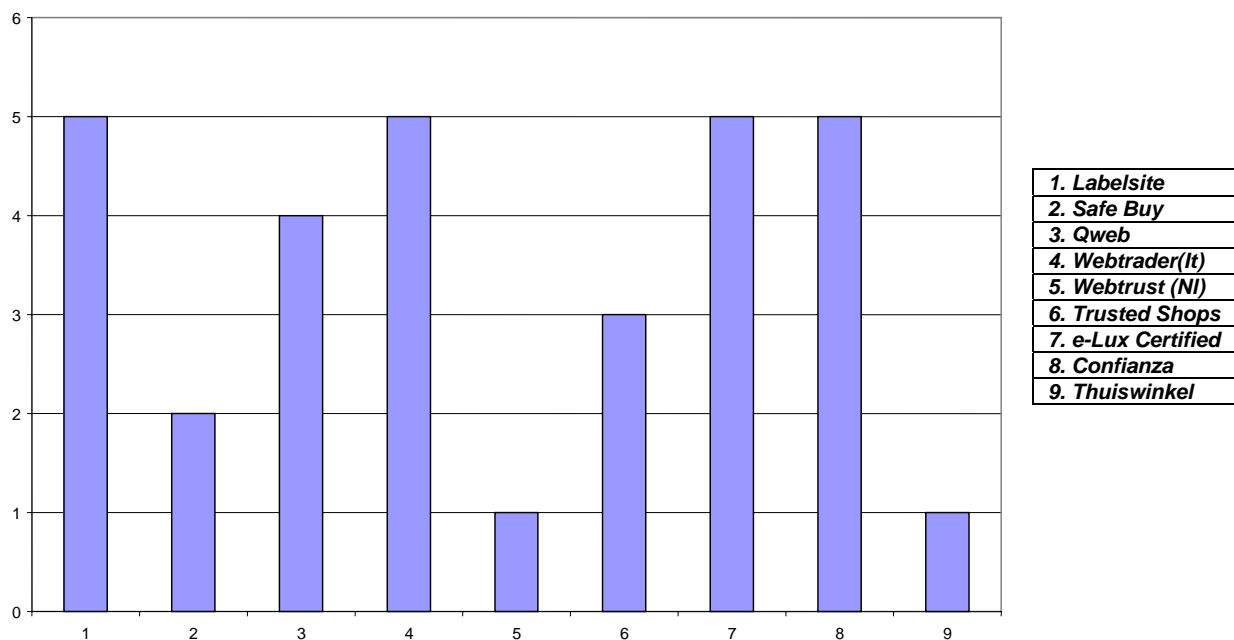
Prior to a transaction becoming a binding obligation (before the conclusion of the contract), merchants should provide consumers with a summary that includes: the terms and conditions of the transaction; the selected payment method; and the option to cancel or affirmatively complete the transaction.

⁸⁰ See article 12 of the code (English version): "If the online shop agrees on the laws of the country where it is based, the consumer protection laws of this country shall apply. Moreover, when selling to consumers based in other countries, the online shop must observe the following additional regulations (see the provided list). In case of discrepancies, the more consumer friendly law shall apply".

This principle of “confirmation process” is an eloquent example of the added value that can be brought by soft law in areas where there are no specific legal requirements as such. In this particular area, the soft-law requirements go further than the too general obligation contained in article 11, § 2, of the e-commerce Directive. This disposition is strictly limited to technical errors and states that : “*the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order*”. Indeed, even if the confirmation process allows in a certain manner (depending on the practical mechanisms put in place by the merchant) to prevent technical errors, its final objective is to ensure the quality of the consumer’s consent.

In this respect, the benchmarking shows that generally most of the codes of conduct tackle this issue (68, 89 %). Nevertheless, this obligation could be formulated or underlined in a more precise and conspicuous manner (e.g., as a distinct subtitle of the code). For instance, in the *Trusted Shops*’ code of conduct, the reference to the confirmation process is “lost” into a general section dedicated to “Price transparency and terms and conditions of payment”. Furthermore, it is formulated in a very ambiguous manner: “*In the event of several articles being ordered the online shop’s order system must, at all times, enable customers to check which articles they have earmarked in which quantity*”⁸¹.

Table 4.5.4.2
Overview of Confirmation process



Nevertheless, some trustmark schemes impose adequate and practical confirmation mechanisms, such as for instance the “double click” mechanism⁸². The *Labelsite*’s code of conduct (Règle 9: Sur les modalités de commandes) gives an adequate example of good commercial practices :

⁸¹ See section 4 of the “Certification criteria/Obligations”, http://www.trustedshops.de/en/shops/obligations_en.html.

⁸² The *Webtrader Italy*’s code of conduct even contains a “triple click” mechanism. See article 4 (Ordering procedure), http://www.soldi.it/webTraderSite/code_uk_it.html: “*The supplier shall use an ordering procedure that limits the chance that the consumer makes an error, such as triple click (...)*”.

“ Faire en sorte que le simple clic sur un produit ou un service ne vaille pas commande.

Ainsi la validation d'une commande doit se faire par au moins deux opérations successives, l'une pour choisir le produit, l'autre pour la validation finale de la commande.

Par exemple :

- 1er clic (ou série de clics) pour le contenu de la commande (panier ou autre...)
- 2ème clic (ou série de clics) pour la validation finale de la commande (modalités et conditions de paiement etc.)

En tout état de cause, le processus de validation doit contenir le récapitulatif complet de la commande et du prix à payer⁸³.

E-platform security

Under this very important topic, we first examine whether codes require merchants to provide information to their customers regarding the security issues and more particularly the security of electronic transactions and payments.

Even if EU instruments cover many aspects related to e-commerce and distance selling, issues related to misuse of payment instruments or the technical security of the payment network⁸⁴, soft law plays an important role here. In particular in view of the direct relation between e-merchants and consumers in this “sensitive” area. This is a very important aspect because consumers’ confidence in internet payment systems is critical to growth of e-commerce.

The development of online payments and the expansion of distance selling could very much depend on the existence of safe and easy payment methods, at a cost level acceptable to retailers and consumers. It may also be important to provide consumers with transparent information on all relevant issues. In this last area, there are still many e-security and e-payment issues that remain unclear to consumers, notably the liability, role and responsibilities of each party⁸⁵. Furthermore, the problem of information remains crucial since many customers continue to perceive themselves as the likely victims should a transaction go wrong. From a legal viewpoint, however, the damage should in reality be borne principally by the trader or the payment-system provider.

Table 4.5.4.3

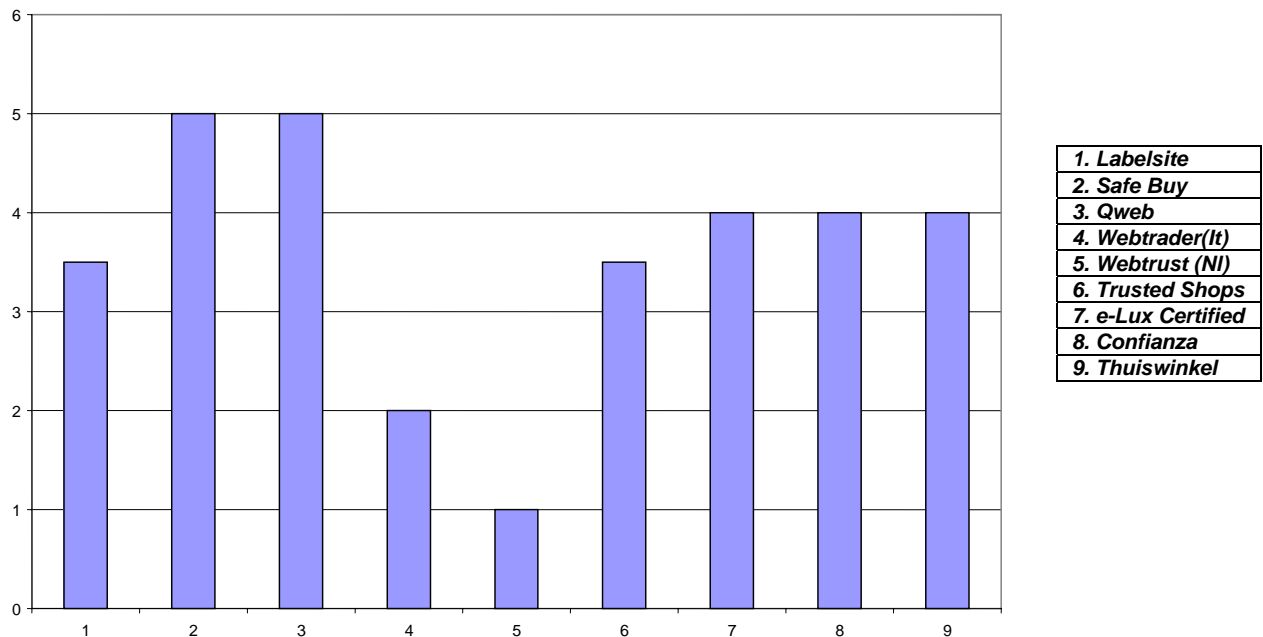
⁸³ In addition, the *Labelsite's* code of conduct inserts an interesting recommendation: « *Le double clic doit s'entendre, par exemple, de la façon suivante :*

- *Après avoir rempli son “panier” en cliquant sur chaque produit, une icône doit être offerte au client avec en dessous une phrase pour dire, par exemple, “oui, je suis d'accord sur le contenu de ma commande”.*
- *Dans un deuxième temps, lorsque le client a communiqué ses coordonnées, choisi son mode de paiement, etc... une deuxième icône doit être offerte pour la confirmation finale de la commande avec en dessous une phrase du type : “oui, je confirme ma commande” ».*

⁸⁴ See the list of EU sources mentioned in the annexed WP 2

⁸⁵ See the special Eurobarometer European Commission, “Issues relating to business and consumer e-commerce”, Executive Summary, March 2004, p. 5, http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_201_executive_summary.pdf: “*In the context of issues of concern to those having used e-commerce, security of payment was still an important issue for 48% of EU15 respondents*”.

Overview of Platform Security



In relation to the issue of transparency, the benchmarking reveals that most of the codes of conduct require merchants to provide information on e-security issues. Nevertheless, the precision of the requirements may greatly vary from one code to another.

In this respect, some codes explain in detail: *SafeBuy's* code states (article 6.2.) that “methods of payment must be as secure as is practicable and the consumer clearly advised of the level of security applicable. If a hyperlink is required to another site with further details of the level of security it should be prominently displayed” and stipulates (article 6.3.) that “the retailer must identify a named individual who is responsible for all aspects of security”. Others are more brief. Luxembourg e-commerce certified’s code only stipulates (requirement n° 35) that “The provider must inform his customer of the existence of a secure payment system”⁸⁶.

We have also analysed whether codes of conduct impose adequate technical requirements related to e-security and more particularly to security of electronic transactions and payments. In this respect, almost the same comments apply to these technical issues. In general, this requirement is met, but there are some great differences in the codes of conduct and therefore in the quality level of the certification process.

Some trustmark schemes provide for specific security audits based on high-level quality standards. This is the case of *Luxembourg e-commerce certified* where applicants have to undergo a double audit. The first one deals with the requirements regarding the provision of information society services⁸⁷. The second one is dedicated to the security of the information system (security of transactions, confidentiality and rules of protection of personal data) and is based on a particular “code”⁸⁸. Depending on the certification level chosen by the

⁸⁶ Eventually, it has to be stressed that *Webtrader Italy's* code of conduct does not include any requirement on this aspect!

⁸⁷ See the “référentiel du certificat qualité Luxembourg e-Commerce Certified”.

⁸⁸ See the “mini-guide de Sécurité des Systèmes d'Information”.

merchant, *Qweb* can also impose specific IT-security standards and recommend the observation of particular technical norms as BS 7799⁸⁹.

Other trustmark schemes do not carry out specific security audits, their codes of conduct generally oblige merchants to implement procedures designed to ensure the integrity, authenticity and confidentiality of data. These procedures should be in accordance with the state-of-the-art and in line with the degree of risk of the concerned application. Nevertheless, in such important matter, codes of conduct should – in addition to their general requirements – make relevant recommendations regarding the particular use of certain technologies⁹⁰.

Customer service

Customer service and contact point

In the framework of the present benchmarking activity, the concept or notion of ‘customer service’ has to be taken in a broad sense. It aims to see whether a code of conduct makes recommendations regarding the implementation of a general contact point for consumers, the accessibility of such a contact point, the means offered to consumers to solve a dispute such as in-house resolution processes and alternative dispute-resolution mechanisms.

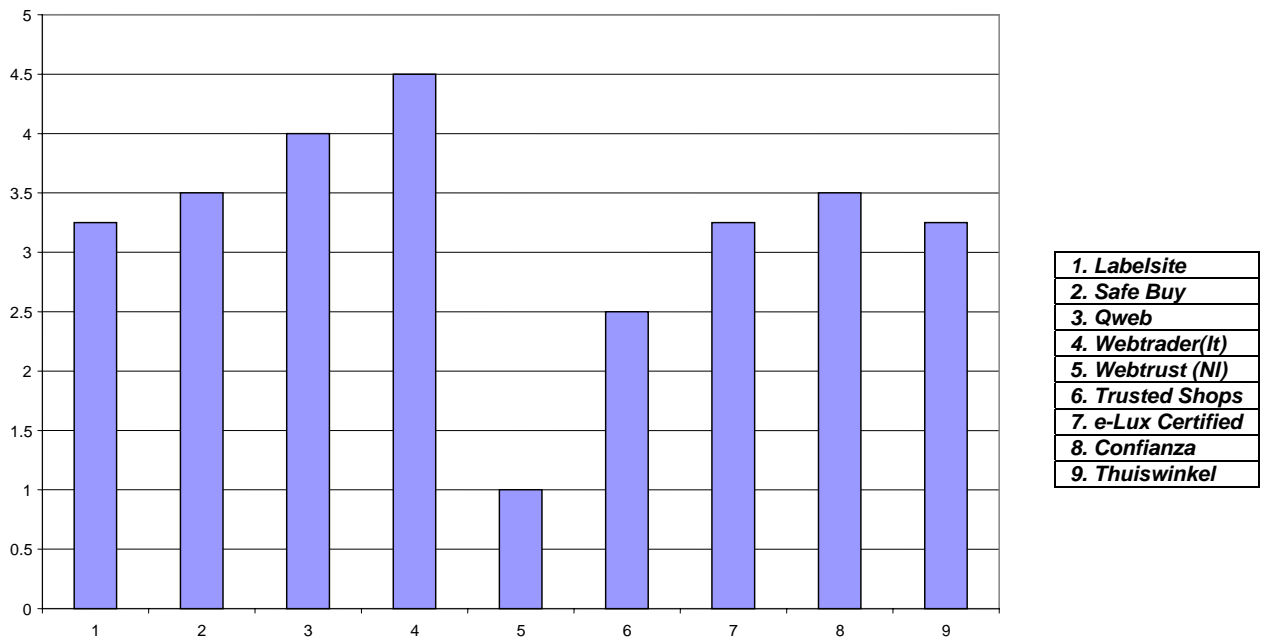
In this sense, customer service deals with the ability of an organisation to constantly and consistently meet the customer’s expectations. In this respect, even if the general outcome is positive (63, 98%), we have observed that some codes only focus on conflicting relationships (complaints procedure). In our opinion, a customer service should not be limited to this single aspect. It can serve to help consumers in matters which are absolutely not connected with a dispute, e.g., asking for information (unsent operating instructions, technical advice), providing feedback, etc⁹¹.

⁸⁹ See entry “What is Qweb mark?”, <http://www.qwebmark.net/english/who.html>: “*Being a three-level certification system, Qweb allows the companies with certified sites to evolve from the one star-level to two or three-stars level, thus increasing their performance in terms of quality and security. Moreover in levels two and three the e-business and e-commerce software is validated in terms of functionality and usability through a series of tests carried out by specialized laboratories*”.

⁹⁰ See the *Labelsité*’s code of conduct (Règle 10) : “(...)Préciser le ou les systèmes retenus et leurs principales caractéristiques, sachant que les systèmes acceptables doivent prévoir un cryptage sur au moins 48 bits. (...)”.

⁹¹ For instance, *SafeBuy*’s code of conduct mainly refers to the customer service (this term being not used as such) under a section entitled “Faults and Disagreements”.

Table 4.5.4.4
Overview of Customer Service



We insist on the fact that codes of conduct should tackle this problem more consistently. This can be done by making a distinction between the different aspects of a customer service and providing clearer and detailed recommendations to the merchants. More generally, trustmark schemes should ensure that companies have the necessary tools and the expertise to satisfy their customers and make the most out of e-business activities.

In this context, trustmark schemes should pay particular attention to the type of targeted adherents. They should bear in mind that all potential subscribers, notably SMEs, do not have the financial and human resources to create and maintain such a service. However, in this case, we advocate that a simple consumer contact point is made available, if applicable in co-operation with other parties.

In the end, and not considering the commercial aspects, the former observations can be justified for at least two reasons:

- § Customer service is first and foremost about quality and relationship building (CMR). Therefore, the promotion of a good customer service will impact on business in a positive manner;
- § Customer service is a valuable instrument for merchants to constantly review and improve their services, notably by assessing every compliment, comment and complaint received;
- § With the connectivity, speed and utility of the internet, we are entering an entirely new field characterized by genuine and meaningful interactions between individuals and companies. Therefore, merchants should adequately use technologies in order to give the consumers the tools they need to overcome many of the traditional obstacles to receive effective feedback.

Complaints procedure and complaint handling

Indeed, more and more consumers or business organisations underline the necessity for merchants to implement internal consumers redress systems. They hold that the vast majority of customer complaints can be resolved in-house if they respond to customer complaints fairly, promptly and in a satisfactory manner.

This general trend can be observed through the enacting of several normative documents (good practices or guidelines) at international level. An outstanding illustration of this trend is the recent document called “*Alternative Disputes Resolution Guidelines*”, sanctioning the agreement reached between Consumers International and the Global Business Dialogue on Electronic Commerce⁹². Both organisations insist on this issue by stating that: “*As a first and preferred remedy in any dispute, Internet customers should be offered access to in-house customer satisfaction systems. Depending on the type of transaction and the nature of the system, such approaches may serve as a valid alternative to alternative dispute resolution (...). In any event, it appears advisable to request that customers direct any complaint first to an in-house customer satisfaction system prior to taking advantage of any ADR mechanism*”.

The analysed codes of conduct are in accordance with this general trend. They require merchants to provide information on the complaints procedure. Nevertheless, some trustmark schemes should impose in a more systematic way guiding principles of a company’s complaints handling and customer redress system.

Such principles could help merchants to implement a redress system that is:

- § objective and clear;
- § credible and supportive to customers;
- § easily accessible;
- § free for customers;
- § providing speedy and equitable treatment;
- § not depriving the customer of any right he would otherwise have;
- § operated with sufficient resources.

Alternative dispute resolution

Under this topic, we have benchmarked whether codes of conduct require merchants to propose to their customers the possibility of alternative dispute resolution and inform them about their participation in such a scheme. In other words, unless full customer satisfaction is guaranteed by in-house systems, customers of merchant websites used for B2C transactions should be notified that the merchant is ready to submit disputes resulting from online transactions to one or more specified ADR system.

According to the code of conduct, information about dispute resolution via ADR should be provided as part of the overall information or as part of the general sales conditions. ADR should be presented as a voluntary option for consumers if a dispute arises, not as a contractual obligation.

⁹² “Alternative Dispute Resolution Guidelines”, Agreement reached between Consumers International and the Global Business Dialogue on Electronic Commerce, November 2003, p. 56, <http://www.gbde.org/adragreement03.pdf>. See also International Chamber of Commerce, “Putting it right – Best practices for customers redress in online business”, November 2003, http://www.iccwbo.org/home/e_business/word_documents/PUTTING-rev.pdf.

For the benchmarking results, we underline that this criterion must be interpreted in parallel with the complaints procedure⁹³ of the trustmark scheme itself. We will comment on this point hereafter. In this respect, we can nevertheless note that metacodes require merchants to inform their customers on the dispute resolution scheme they adhere to. But it is not totally surprising that this information concerns in many cases the adherence to the complaint and/or ADR process of the trustmark scheme⁹⁴.

From a more abstract point of view, codes of conduct should play a role in educating consumers on the alternative dispute processes and their rights under such a system. One way to do this, is to include information on ADR as part of the purchase agreement. In this way, the consumer is required to acknowledge that he is aware of the ADR process before a transaction can be executed and becomes legally binding.

Protection of children

The evaluated trustmark schemes pay a positive attention (65,18%) to the protection of minors and other vulnerable persons. Even though minors cannot - in principle - be engaged in a legally binding act, we notice that they become more and more the object of providers of information society services and (unfair) commercial communications.

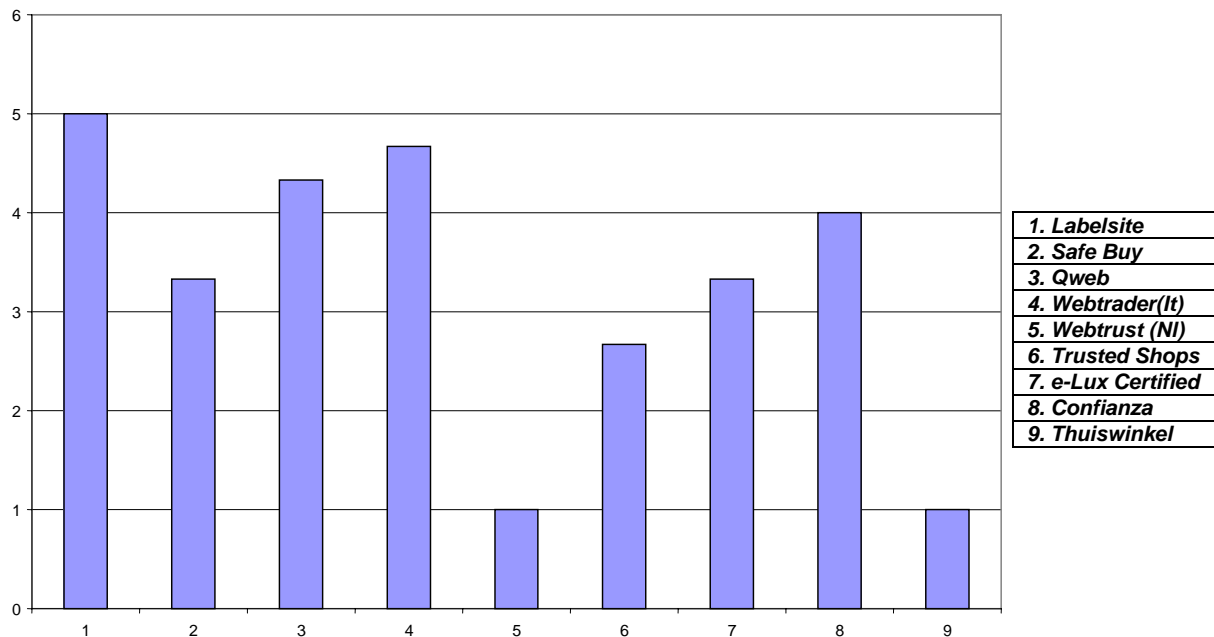
From a hard-law point of view, the underlying problems are somewhat underestimated because these persons *de iure* cannot execute binding legal obligations. However, they *de facto* participate in, and benefit from, the Information Society. This could be a reason why some trustmark schemes pay less attention to this problem.

In absence of a comprehensive and adequate regulatory framework regarding the online protection of minors, some trustmark schemes demonstrate that they make a valuable contribution in this area and contemplate the hard-law provisions.

⁹³ To be understood in a broad sense.

⁹⁴ See *infra*, phase 6 dedicated to “complaints procedure”.

Table 4.5.4.5
Overview of Child Protection



4.5.5 Phase 5: Proactive monitoring

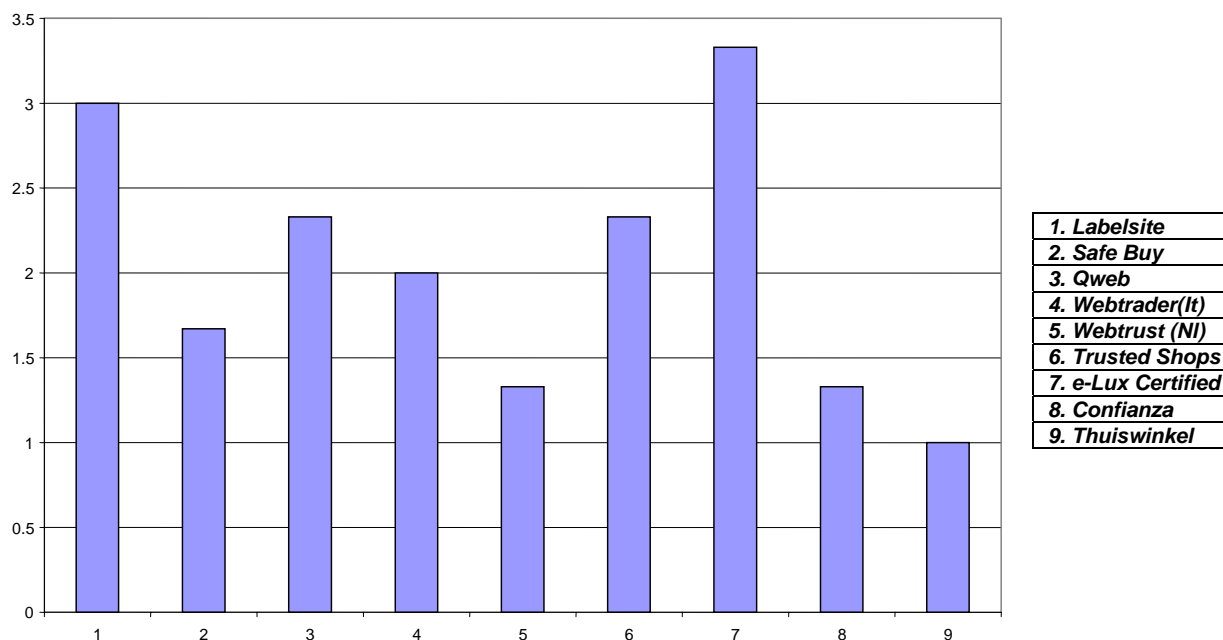
Considering the methodology used for the benchmarking, one can consider that the results related to the quality of proactive monitoring depend on the available information published on the website. In this regard, we have observed the lack of transparency of metatrusted mark schemes. Nevertheless, some interesting conclusions can be drawn from the benchmarking of this field.

- § As regards the **fairness** of the monitoring, most trustmark schemes do not seem to monitor their subscribers on an independent basis. It means that the monitoring does not rely on the intervention of an independent third body (external to the scheme) nor to a specific body operating inside the scheme that should, for instance, be composed on the basis of a balanced representation of the interested stakeholders (*notably* businesses and consumers). In most cases, there is no “separation of powers” as such, and one single body is in charge of all activities of the scheme⁹⁵.

Furthermore, due to the lack of information in this area, it is difficult to see whether trustmark schemes monitor their subscribers in a non-discriminatory manner by random checks or by systematic monitoring of all the certified merchants.

⁹⁵ There are of course some exceptions. For instance, *Luxembourg e-commerce certified* has a “Comité de certification”, where consumers are represented, which is a “*structure indépendante, regroupant des compétences multiples et des intérêts divers, apporte une vision et une expertise supplémentaire qui garanti le respect des règles déontologiques du processus de certification*”.

Table 4.5.5.1
Overview of Proactive monitoring evaluation



§ Regarding the **effectiveness** of the monitoring, most trustmark schemes do not seem to put in place all the possible mechanisms to establish and monitor compliance with trustmark-scheme specifications. Even if they often refer to the method of “mystery shopping” (carry out purchase check on the certified websites with no prior notice), they do not mention other methods such as regular reporting requirements on code subscribers, specific audits, etc.

In parallel, if the checks reveal any non-compliance with the requirements of the code of conduct, trustmark schemes should systematically oblige their subscribers to implement corrective actions.

The regularity of checks may vary considerably from one trustmark scheme to another. Some trustmark schemes limit themselves to “regularly” sample sites⁹⁶, while others put in place very precise timeframes⁹⁷.

A rapid comparison between *Qweb* and *Luxembourg e-commerce certified* – which have the same validity term of the trustmark seal of 3 years – illustrates the difference between the frequency of the monitoring. If both certification bodies carry out a “surveillance audit” of subscribers at least on a yearly basis, *Qweb* makes front office checks every three months whereas *Luxembourg e-commerce certified*'s subscribers are submitted at least to one purchase test every year. This example does not even allow the conclusion that the regularity of checks depends on the duration of the granted trustmark seal.

⁹⁶ See article 1.5. of *SafeBuy*'s code of conduct.

⁹⁷ See the monitoring table provided by *Qweb* in its FAQs, <http://www.qwebmark.net/english/who.html>.

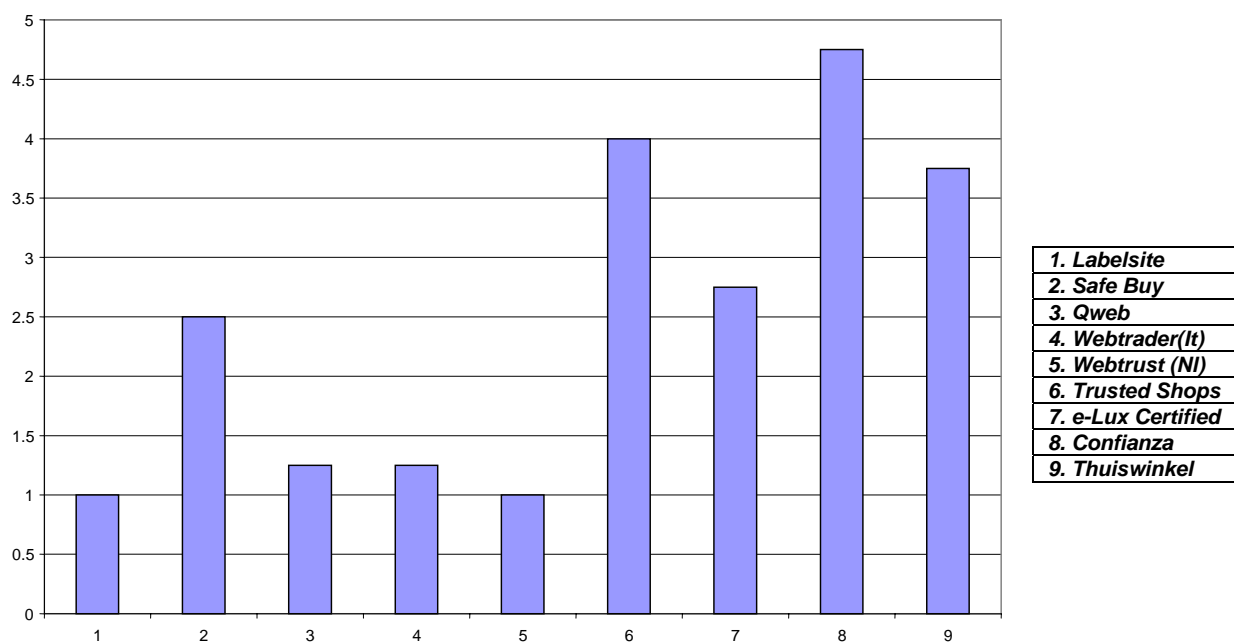
4.5.6 Phase 6: Complaints procedure

To avoid confusion, it must be specified that the term “complaint” refers in this section to the situation where a dispute between a merchant and a consumer is not mutually resolved. For this reason, the dispute has escalated to a complaint lodged with a third party. This third party can be the trustmark scheme itself or a third party.

Effective and efficient consumer remedial mechanisms are important to build trust. First, internal company complaint handling procedures, conspicuously identified on a company’s website, are the appropriate first step for a consumer complaint. When consumers are unable to resolve their dispute directly with a company, they should have the possibility to turn to a third party.

In this respect, the benchmarking reveals that most the trustmark schemes offer mechanisms to deal with complaints regarding non-compliance with the trustmark requirements. Nevertheless, the nature and also the quality of those mechanisms may vary substantially between trustmark schemes.

Table 4.5.6.1
Overview of Complaints procedure evaluation



Accessibility and convenience

Consumers must be fully aware of the existence of dispute-resolution mechanisms. While it is desirable that consumers have knowledge of these systems prior to purchase, it is critical that this information be available at the time a dispute arises. In this respect, the benchmarking shows that trustmark schemes should make the redress information available to consumers in a more direct user-friendly manner. Some trustmark schemes’ websites do not even provide any information or any specific entry for this.

Accessibility not only means that the mechanism can be called upon when needed. It also implies that there are no unreasonable barriers to access. In this respect, the consumers' process of contacting the trustmark scheme to ask for assistance in resolving a dispute should be highly visible and easy to use. This is not always the case.

An on-line complaint form is one way to do this. It can be made accessible through the dispute resolution body's or the merchant's website. The benchmarking shows that just a few trustmark schemes use this type of electronic complaint form. However, they should take advantage of the opportunities offered by new technologies; by using the internet, speed and efficiency in handling the dispute will be increased⁹⁸.

More generally and instead of providing a general contact point ("contact us", "feedback") without any information on the complaints procedure⁹⁹, trustmark schemes should make efforts to improve the accessibility of a dedicated complaints procedure.

Quality of the complaint – dispute-resolution process

The quality of the complaints procedure largely depends on the type of mechanism chosen by trustmark schemes. The benchmarking reveals that – unlike the categorizations of the methodology, where a distinction is made between complaints procedure (internal) and alternative dispute resolution (external) – trustmark schemes do not generally propose a "double-phase redress system" as such. It means that either they provide their own dispute-resolution services (internal complaints procedure) or they collaborate with a third body (external ADR body), but rarely both¹⁰⁰.

In this context, *SafeBuy* can be viewed as an exception that merits our attention. This trustmark scheme has the following dispute-resolution system¹⁰¹:

1. In the event the merchant and consumer cannot agree on the resolution of a complaint, the merchant must advise the consumer of any relevant complaints body, regulator or ombudsman.
2. In parallel, the merchant must also advise the consumer of the *SafeBuy* mediation procedure.
3. Finally, in the event of the merchant's own complaints procedure and the *SafeBuy* mediation procedure being unsuccessful in resolving the complaint, the merchant agrees that the consumer has the right to arbitration under the EEJ-NET scheme of the Chartered Institute of Arbitrators.

In this context, one has to bear in mind that the distinction between internal complaint and alternative dispute-resolution processes is not always very clear.

⁹⁸ But consumers should not be limited to internet access to the redress system and they should be able to submit their complaint by letter, telephone or any other means of communication.

⁹⁹ See for instance, *Labelsite's* website that only provides for an entry "Vos commentaires" which automatically activates the visitor's e-mail editor.

¹⁰⁰ On a methodological point of view (benchmarking), it implies that the complaints procedure has been considered in a broad sense. In case of involvement of a third resolution body, the scores have been attributed under the criterion related to the "quality of the complaints procedure".

¹⁰¹ See article 5, §§ 3 to 6 of *SafeBuy's* code of conduct, <http://www.safebuy.org.uk/codeofpractise.htm>.

Table 4.5.6.1
Comparison of Dispute Resolution processes

Trustmark schemes	Internal ADR	External ADR
1. Labelsite	[see Euro-label] ¹⁰²	EEJ-Net
2. SafeBuy	Safebuy mediation	Chartered Institute of Arbitrators
3. Qweb	–	European Network of Arbitration chambers
4. Webtrader Italy	Webtrader/Altroconsumo	–
5. Webtrust NL	–	–
6. Trusted Shops	Money charge back guarantee	–
7. Lux. E-commerce certified	Certification body (SNCH)	
8. Confianza Online	[AECE Mediation] ¹⁰³	Jurado de la Publicidad – Junta Arbitral Nacional de Consumo
9. Thuiswinkel	Stichting Geschillen Commissie	

As to the fairness of the process, the observations formulated above must be taken into account. In any case, the redress mechanisms must be perceived as treating both parties at least as equitably and fairly as a formal government administrative or legal procedure would. Consumer dispute mechanisms must have structure, rules and procedures that ensure that all parties' rights are protected, and that every aspect of the mechanism operates with regard to the parties' rights to due process¹⁰⁴. Obviously, one can expect more independence and neutrality from the intervention of a "real" third party resolution body

The results regarding the effectiveness of the process can considerably vary from one trustmark scheme to another. This can be partly explained by the lack of transparency in this area. Some trustmark schemes only vaguely address dispute-resolution issues, while others make a detailed procedure available on their website. This is for instance the case for *Confianza Online*¹⁰⁵ and *Thuiswinkel*¹⁰⁶.

In this view, it must be underlined that *Confianza Online* seems to be the sole trustmark scheme making explicit reference to the principles contained in EU Recommendation 98/257/EC on the principles applicable to the bodies responsible for out-of-court settlement

¹⁰² *Labelsite's* website does not provide any information on the complaints procedure, except a laconic and ambiguous reference among the listing of the competences of its "Comité d'habilitation" (Examen des rapports de réclamations).

¹⁰³ *Confianza Online* firstly proposes to solve the complaint through AECE's mediation (seven working days). But it must be underlined that even if the mediation is handled by AECE (which is one of the promoting associations of the trustmark scheme), this mediation cannot be considered an internal complaints procedure as such.

¹⁰⁴ The principle of fairness should also ensure that the complaints procedure is open to all consumers, without any discrimination. In *Webtrader Italy's* scheme, members of *Altroconsumo* are only able to lodge a complaint: "Se sei socio di Altro Consumo e hai una controversia con un'impresa che vanta il nostro logo oppure quello rilasciato da un'altra organizzazione di consumatori della rete Web Trader, contatta il nostro servizio associati".

¹⁰⁵ See entry "Tramitación de reclamaciones", <http://www.confianzaonline.org/>.

¹⁰⁶ See entry "Geschillenbeslechting", http://www.thuiswinkel.org/onderdeel/consumenten/thuiswinkel_waarborg/over_geschillencommissie.asp?lokatie=homepage.

of consumer disputes¹⁰⁷. In this respect, trustmark schemes should more often draw their inspiration from this instrument and from Recommendation 2001/310/EC. The latter Recommendation deals with the principles for out-of-court bodies involved in the consensual resolution of consumer disputes.

Furthermore, the link between trustmark schemes (and their respective complaints procedures) and the European Extra-Judicial Network for cross-border dispute resolution (EEJ-Net)¹⁰⁸ should be better developed¹⁰⁹. In this respect, trustmark schemes should make a systematic reference to the competent *Clearing House*.

Finally, the results of the dispute-resolution process should be visible to both parties and to the public at large. This will probably reinforce the company's interest to act in a responsible manner and its interest to avoid damaging its reputation. The publication of the outcome of cases does not require the publication of the whole set of proceedings, communications and documentation. Publication can only cover certain types of documents for a certain time frame, the case being with the consent of the parties concerned. This could be clearly stated in the policy and service agreement.

4.5.7 Phase 7: Enforcement

Fairness

For trustmark schemes, fairness means in particular that their funding and board structure should be neutral. In practice, the benchmarking reveals that this objective is not always easy to achieve. Merchant members usually pay directly for the provided services, e.g., a membership fee. This direct financial link between the trustmark scheme and its members may imply a conflict of interest, notably when sanctions have to be enforced.

This situation could be counterbalanced by additional safeguards, such as for instance an independent third body supervising the scheme and the representation of consumers on the board of the scheme (surveillance committee). Unfortunately, the existing schemes rarely implemented these additional safeguards.

In this context, trustmark schemes should create a kind of "surveillance committee" as an independent monitoring and compliance body that guarantees the neutrality and impartiality of the scheme¹¹⁰.

Such body could have the following competence: i) managing the complaint contact address which provides details of any problems facing both merchants and consumers; ii) deciding which actions are needed vis-à-vis companies which do not comply with their contractual duties; iii) interpreting the code of conduct and amending it when necessary. All legal

¹⁰⁷ See code of conduct, pp. 4-5 : "*Este sistema de resolución de conflictos está inspirado en los principios de independencia, transparencia, contradicción, eficacia, legalidad, libertad de elección y derecho de representación por parte del consumidor, que coinciden plenamente con los principios exigidos por las autoridades comunitarias para el reconocimiento de los mecanismos extrajudiciales de resolución de controversias con los consumidores, plasmados en la Recomendación 98/257/CE de la Comisión Europea*".

¹⁰⁸ See <http://www.eejnet.org/>.

¹⁰⁹ Few trustmark schemes refer to the existence of this specific network.

¹¹⁰ See, for instance, the CCform initiative, <http://www.complaintsplatform.com/>.

entities, be they private or corporate, could request this body to intervene if they notice a violation of the code.

Besides such organisational conditions, trustmark schemes should pay attention to the transparency and the fairness of the procedure of enforcement itself. The benchmarking shows that trustmark schemes lack transparency. They generally limit themselves to inform about the possibility that the trustmark seal will be withdrawn, without providing any indications on the different hypotheses of withdrawal or the decision's procedure¹¹¹.

Effectiveness

- § Trustmark schemes do not generally provide statistics on the removal of trustmark seals from certified websites. In the best scenario, some provide raw figures about the number of seals issued or sometimes the number of disputes dealt with. However, this makes it very hard to have a practical overview of the effectiveness of self-regulatory site labelling. Are the trustmark scheme's requirements only statements of aspiration or should they be perceived as more meaningful because the issuing party has the resources - and will - to effectively police the trustmark?

Nevertheless, the benchmarking allows formulating some interesting observations.

In most cases, trustmark schemes provide for the withdrawal of the trustmark when the subscriber fails to take action to comply with the trustmark requirements. Although this can be reassuring to some people, it can also create some difficulties when a drastic measure like this is the one and only sanction that can be undertaken against subscribers.

Trustmark schemes should therefore see this sanction as the ultimate step of a gradual coercion-scheme. The lesser sanctions being, in accordance with the gravity of each case and the damages caused, e.g. a warning, a reproach and a temporary withdrawal of the logo. These sanctions could finally lead to the definitive exclusion from the system. Such a system could without a doubt ensure the proportionality of the enforcement as recommended by the European Trustmark Requirements (ETR)¹¹².

In addition to self-regulatory sanctions and in the event the positive law is infringed, the trustmark scheme could, for instance, decide to report the merchant concerned to the relevant public authority.

- § As mentioned above, the benchmarking reveals that in most cases trustmark schemes do not mention or provide for the publication of the sanctions imposed on merchants¹¹³.

¹¹¹ For instance, one has to question whether the subscriber should have a right to appeal against the decisions of the trustmark scheme. Most of the trustmark schemes do not seem to offer this possibility.

¹¹² See section 8, al. 3 and 4, of ETR: "A list of *dissuasive and proportionate* sanctions should be established, which could include information to the media and financial fines."

¹¹³ *Confianza Online* seems to be the exception in this area. It provides for the publication of the results of the complaints procedure on the website. "Once the *Jurado de la Publicidad* or the *Junta Nacional Arbitral de Consumo*'s resolution has been reported to the interested parties for their compliance, it will be placed on the *CONFIANZA ONLINE*'s web page and in *AUTOCONTROL*'s and *AECE*'s sites and other resources as well. In particularly serious cases, *AUTOCONTROL* and *AECE*'s

The question arises to what extent publication of sanctions (or ADR results) is practicable. It is to be expected that merchants will oppose the publication of results. In practice, most trustmark schemes do not seem to implement publication of sanctions and, of course, there is no legal obligation to do it.

Nevertheless, one has to wonder whether such publication could bring a real pressure on subscribers, e.g., to avoid damage to the business reputation that results in customer loss.

- § Eventually, the benchmarking also reveals that most trustmark schemes do not propose specific “remedies” to consumers as money-back guarantee¹¹⁴ or escrow services¹¹⁵. In this respect, the question arises whether trustmark schemes should not provide for this type of mechanism in addition to the traditional ways of enforcement (sanctions, dispute resolution). There is no doubt that such specific protection mechanisms will enhance consumer confidence in electronic commerce more than the consumers’ simple awareness of the potential sanctions that can be imposed on negligent merchants.

In this context, it must be underlined that both types of enforcement (sanctions imposed on merchants – compensation of consumers) do not exclude each other¹¹⁶.

4.5.8 Phase 8: Relationships with protagonists

General relationships

The benchmarking aims to examine whether trustmark schemes implement adequate mechanisms in order to enhance confidence in their relationships with all the interested parties.

First, the benchmarking reveals that all trustmark schemes’ websites provide for a contact point to encourage feedback from interested parties. According to the methodology the implementation of a contact point has been considered a *must-have* criterion. Nevertheless, the character of this contact point can considerably vary from one trustmark scheme to another. Some have multiple contact points depending on the type of request, some have a specific feedback form. Others only offer a website’s entry that directly activates the visitor e-mail editor.

respective Boards of Directors can decide how to publish it actively. In any case, publication will always protect the anonymity of the complaint’s personal data when he / she is an individual consumer, in such a way that the name and other complainant’s personal data will not appear in the published text of the resolution”. See <http://www.confianzaonline.org/reclamaciones/resoluciones.php>.

¹¹⁴ *Trusted Shops* is the exception.

¹¹⁵ Escrow service means holding payment until consumers are satisfied. Some companies offer escrow services through which a third party (sometimes for a fee) can hold money until the consumer gets the goods or services he ordered or is satisfied with its purchase.

¹¹⁶ For instance, *Trusted Shops* could additionally propose a dispute-resolution process for all the problems that are not directly covered by its money-back guarantee (this guarantee aims to protect consumers in three cases: non-delivery of goods, non-refund after returning goods and credit card fraud).

For the additional services offered on the website, the benchmarking shows that efforts should be made in this area¹¹⁷. Some trustmark schemes' websites do not even propose "Frequently Asked Questions" which are in fact a very useful method to make information understandable for first-time visitors. Trustmark schemes should also more systematically provide for "interesting hyperlinks" that refer for instance to EU regulations or initiatives, law portals, search engines, relevant organisations, etc.

Relationships with consumers and business

As to the validity of the issued trustmark seals, some trustmark schemes simply insert a link to their website and leave the consumer the burden to search the information that will enable him to verify whether or not the webtrader is certified¹¹⁸. Considering the available existing technologies, it would be welcomed if this practice is abandoned.

In this context, trustmark schemes should allow direct verification of the validity of certification through a click on the displayed trustmark seal. Such a click should make a specific window appear which includes relevant information such as the merchant's identification data, its representatives and of course the validity period of the certificate. *Trusted Shops* gives a good example of such practice. Figure 4.5.8.1 gives an example of what appears when one clicks on the logo displayed on the merchant's website.

Moreover, it has been observed in many cases¹¹⁹ that subscribers do not always display the logo on their website in a conspicuous manner. Trustmark schemes should pay more attention to this aspect and set up adequate checks!

Regarding the communications strategies, some trustmark schemes should perhaps more systematically include in the website's architecture an entry especially dedicated to businesses in order to promote their services and provide for more specific information¹²⁰.

Finally, critical observations regarding confidentiality and data-protection issues (data transferred both by merchants and consumers to trustmark schemes) have already been made in the section dedicated to the first phase of the life cycle¹²¹.

¹¹⁷ Nevertheless, some interesting and original additional services are proposed by some trustmark schemes. For instance, *Thuiswinkel* informs about the results of the "Nationale Thuiswinkel Awards" which in particular aims to reward quality webtraders. *Trusted Shops* offers an up-to-date "news entry" that gives useful information.

¹¹⁸ This is for instance the case for *Webtrader Italy* and *Confianza Online*.

¹¹⁹ This observation not being as such part of the methodology.

¹²⁰ See for instance *Thuiswinkel's* website.

¹²¹ See the paragraph dedicated to "security and privacy".

Figure 4.5.8.1
Validity of certification

Trusted Shops Certificate

Trusted Shops is the first Seal of Approval for online shops with an integrated money-back guarantee for online shoppers backed by the Atradius Insurance Group, one of the leading industrial insurers worldwide.

1. Quality guaranteed by our strict certification criteria:
Atelco fulfils the criteria for the Trusted Shops Seal of Approval.
2. Reliability through transparency and consumer protection measures:
Atelco is obliged to meet the highest requirements for data security and delivery.
3. Security through the money-back guarantee:
You can register for the money-back guarantee from Atradius and be insured against non-delivery, non-refund due to returns, and liability for credit card fraud. The online shop assumes all costs for the guarantee.

Please note that money-back guarantee is limited to € 2,500.- (EUR) per purchase according to the Trusted Shops Guarantee Conditions.

Online Retailer Identification

Atelco

Internet address

www.atelco.de

Status

valid

Contact

Gewerbepark Möhnensee, 59519 Möhnensee

Germany

Tel. +49 (0)2924 - 9900

Fax +49 (0)2924 - 994400

versand@atelco.de

Shop Owner

A TELCO Computer Event GmbH

Gewerbepark Möhnensee, 59519 Möhnensee

Commercial Register

Amtsgericht Arnsberg, HRB 5469

Authorized Representative

Ralf Schwalbe

Approved on

01.07.2002

Validity of certificate

from

01.07.2002

to

30.06.2005

5 Commercial viability analysis on trustmark schemes

5.1 Introduction

This chapter analyses the commercial viability of the selected trustmark schemes (see Section 2.3). The analysis is based on a theoretical framework that defines baseline organisation models and a financial model. By means of this model, the business models used in practice and the financial models are assessed. For the financial assessment, a start-up phase (i.e., a period of time spent on preparatory work before trustmarks can actually be issued) and an operational phase are distinguished. This chapter ends with discussing the critical success factors that are identified by the selected trustmark-scheme organisations.

5.2 Theoretical framework on trustmark-scheme business models

For the purpose of this analysis, the trustmark-scheme business models are assessed from an organisational and financial perspective. Three baseline organisation models are defined i.e., a stand-alone trustmark scheme, a trustmark scheme based on a hierarchy and trustmark schemes that operate in a horizontal network. The financial model includes different cost modules and revenue streams that are specific for a trustmark scheme's start-up phase and its operational phase. A combined organisational and financial model allows a more detailed assessment of the business models found in practice.

5.2.1 Baseline organisation models

Theoretically, the following three types of trustmark-scheme organisation models can be distinguished:

- § *Stand-alone organisation model* – The trustmark scheme is operated by a single entity that acts independently from other trustmark schemes. This entity is either created by a new or by an existing organisation or a combination of organisations. It manages the scheme, while certain functions, such as dispute resolution, may be performed by a third party.
- § *Hierarchical organisation model* – The trustmark scheme is operated by several entities, often covering distinct geographical domains, under the authority of a higher level entity according to a common set of rules. Each of these individual entities are either created by new or by existing organisations or a combination of organisations.
- § *Network organisation model* – The trustmark scheme is operated by several entities, often covering distinct geographical domains, in a horizontal network according to mutually recognised sets of rules. Each of these individual entities often are created by an existing organisation or a combination of organisations.

5.2.2 Financial model

The financial model is based on two separate components, on the one hand the costs made and on the other hand the revenue. For a more detailed analysis, different cost modules are defined as well as different options to generate revenue streams. In addition, a distinction is made between the start-up phase and phase where the trustmark scheme is fully operational.

Cost modules start-up phase:

- § *Costs to get the initiative started and to create an organisation* – For an initiative to get started, investments need to be made in terms of creating stakeholder support and an organisational infrastructure: relevant parties need to be visited, meetings need to be held, the organisation itself needs to be set up, including all the legal and communication aspects. The cost of this depends highly on the approach and the willingness of parties to work together. A staff of two people, an office, cost of a board, travelling costs and third party advice seem to be the bare minimum.
- § *Costs to create a code of conduct* – An important building block of a trustmark scheme is a set of rules, usually in the form of a code of conduct, including the approval criteria and enforcement mechanism. Apart from the fact that defining a code of conduct requires specific legal and technical expertise, the process of creating and agreeing on a set of criteria is a highly political process and often very time consuming. Typically, an expert group containing delegates of all primary stakeholders and legal and technical experts drafts these criteria. The time and costs required for this exercise depends on the number of parties involved and the willingness of parties to work together. One possibility to reduce costs, however, is that parties agree on an existing code.
- § *Costs to launch a brand* – A trustmark scheme's success depends on its visibility with business as well as consumers. Therefore it is necessary for its logo to have a strong brand. A high brand recognition with a broad variety of businesses and consumers requires communication through various media channels and therefore can be very costly. The amount of costs depend on whether an entirely new (co-)brand or an online version of an existing brand is used.

Cost modules operational phase:

- § *Permanent organisational costs* – The minimum organisational costs include personnel, office, services from third parties and other (travel etc.).
- § *Permanent marketing costs* – Once a brand has been created, it requires permanent marketing investments to retain or increase brand recognition. Cutting down on marketing, means less visibility and thus less brand recognition. If a trustmark scheme is not prepared to invest a substantial part of its budget in marketing, all the other investments need to be reconsidered for the effect is then very little. Costs for marketing vary widely depending on the ambitions of the trustmark scheme.
- § *Permanent enforcement costs* – Once a trustmark initiative is established and websites have been approved, the criteria must be enforced. Enforcement mechanisms such as permanent monitoring for compliance, corrective measures and/or a dispute settlement procedure need to be provided. The operation of the enforcement mechanisms may require third party legal and technical specialists.

Revenue streams start-up phase:

- § *Project subsidy* – A once-only subsidy, intended specifically for a project related to setting up the trustmark scheme. The revenue stream can be provided by the government, but also by a private organisation.
- § *Permanent subsidy* – Revenue based on structural financial support. The revenue stream can be provided by a public body or private organisation.
- § *Sponsorship* – A once-only donation without any specific requirement. Typically, the revenue stream is provided by a private organisation, for example as investment of the founding organisation(s) or future trustmark users.

Revenue streams operational phase:

Also during the operational phase, revenue can be generated through project subsidy, permanent subsidy and sponsorships. In addition, the following revenue streams can be defined:

- § *User fees* – Users pay fees for compliance audits and or entrance/license fees. These fees can be fixed or variable based on a for example annual turn-over or number of employees. Often, user fees are paid on an annual basis.
- § *“Polluter pays”* – Users of trustmark schemes that generate the most handling, for example as a result of unresolved consumer complaints, pay pro rata.
- § *Other* – Any other possibility.

For the purpose of assessing the financial sustainability of a trustmark scheme, two financial key-performance indicators will be used. The first indicator is that a trustmark scheme generates at least as much revenue as it incurs costs. The second indicator used is the moment in time where the break-even point is reached. A reasonable break-even point not too far away in time is needed to prove the commercial viability of the scheme. Depending on the realisation of the individual trustmark scheme’s business case, a break-even point can be reached at a certain moment in the operational phase, but may also be achieved during the start-up phase already. For the purpose of analysis, a reasonable point in time is defined as less than 2 years. Table 5.2.1 provides an overview of the financial model.

Table 5.2.1
Financial model

	Costs	Revenue
Start-up phase	<ul style="list-style-type: none"> § Costs to get the initiative started and to create an organisation § Costs to create a code of conduct § Costs to launch a brand 	<ul style="list-style-type: none"> § Project subsidy § Permanent subsidy § Sponsorship
Operational phase	<ul style="list-style-type: none"> § Permanent organisational costs § Permanent marketing costs § Permanent enforcement costs 	<ul style="list-style-type: none"> § Project subsidy § Permanent subsidy § Sponsorship § User fees § “Polluter pays” § Other

5.3 Business models used in practice

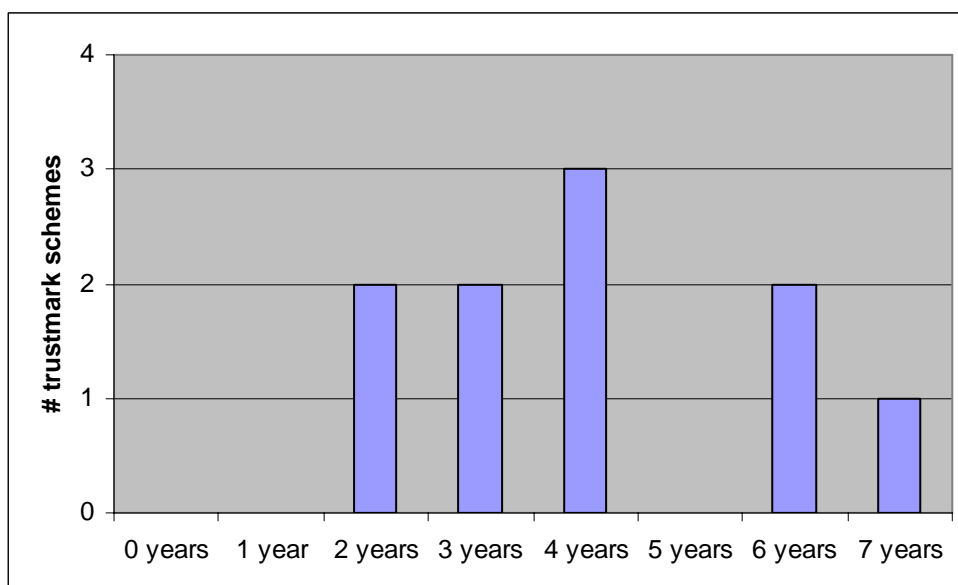
The theoretical model can now be used to assess the business models of the selected trustmark schemes (see Section 2.3 and Annex 7.1). An assessment of the organisation models is mainly made through desk research and partly through a telephone questionnaire. The financial assessment is based on telephone interviews with each individual trustmark scheme. All identified trustmark schemes have responded to the questionnaire. Some trustmark schemes could not or did not want to provide answers to all questions, in particular with regard to particular financial data. Annex 7.5 includes the questionnaire used for these interviews.

5.3.1 Organisation models in practice

For each trustmark scheme, it was assessed to what extent their organisation can be categorized as one of the baseline organisation models. The assessment has shown that some trustmark schemes have a mixed or hybrid model. Annex 4 provides an overview of the assessment results, including a more detailed description of the trustmark scheme's organisation profile.

As can be learned from Annex 4, all assessed trustmark schemes are still operational today except the Web Trader initiative. With more than 7 years of operation, BBBOnline is the oldest trustmark scheme. Euro-label and WebTrust have been around for more than 6 years. Trusted shops, TrustUK, and QWeb more than 4 years. Thuiswinkel and Luxembourg e-commerce certified have been operational for about 3 years and with 2 years, Confianza Online is the youngest initiative. Web Trader ceased operation after 2 years. Figure 5.3.1.1 provides a graphical overview of the operational period of the assessed trustmark schemes.

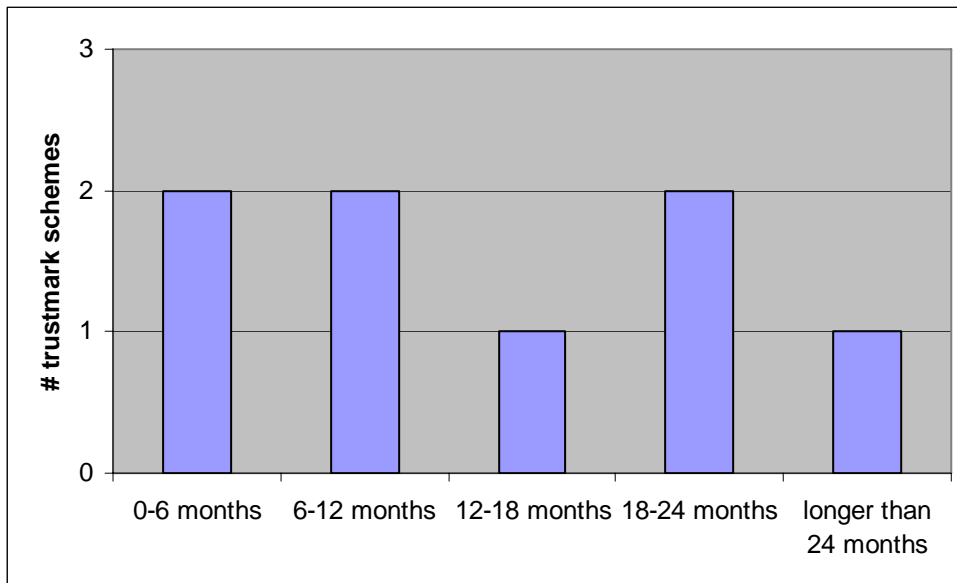
Figure 5.3.1.1
Operational period trustmark schemes



5.3.2 Start-up phase

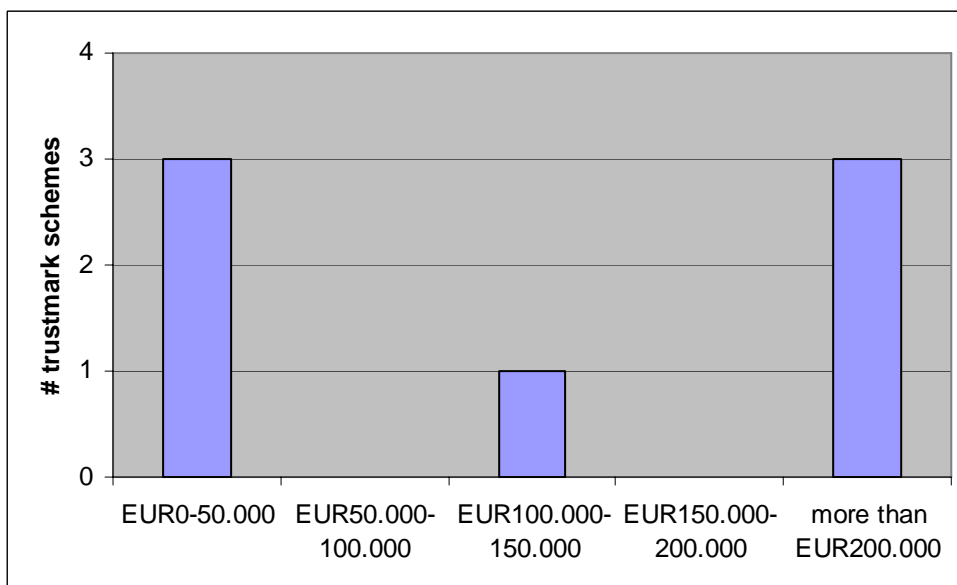
Of the assessed trustmark schemes, all but Thuiswinkel and WebTrust distinguished a start-up phase and an operational phase. The duration of the start-up phase varies per trustmark scheme (see Figure 5.3.2.1).

Figure 5.3.2.1
Start-up period trustmark schemes



§ Total costs start-up phase

Figure 5.3.2.2
Total costs start-up phase

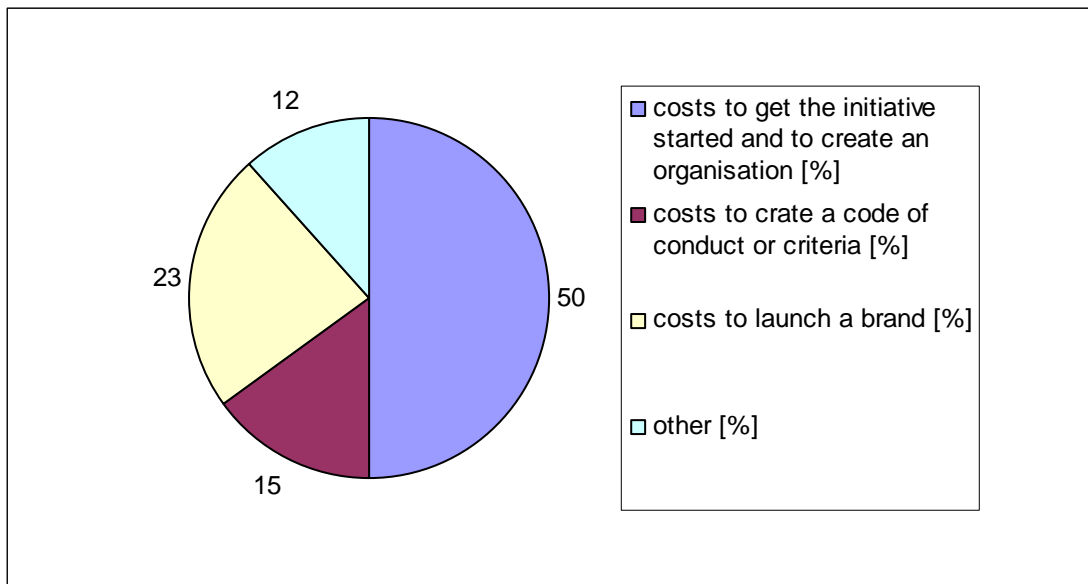


The total costs made during the start-up phase also vary per trustmark scheme. They depend on the individual business cases and the duration of the start-up phase. Of the eight trustmark schemes that indicated to distinguish a start-up phase, seven provided information on the total costs. An overview of these cost is presented in Figure 5.3.2.2.

§ Costs break down

The total costs of the start-up phase as specified in the paragraph above can be broken down into several cost modules. Figure 5.3.2.3 provides a cost break down in percentages of the total costs made during the start-up phase, based on seven trustmark schemes. As can be concluded, in general half of the start-up budget is spent on organisational costs, while costs to launch a brand add up to about a quarter. Fifteen per cent of the budget is spent on the creation of a code of conduct.

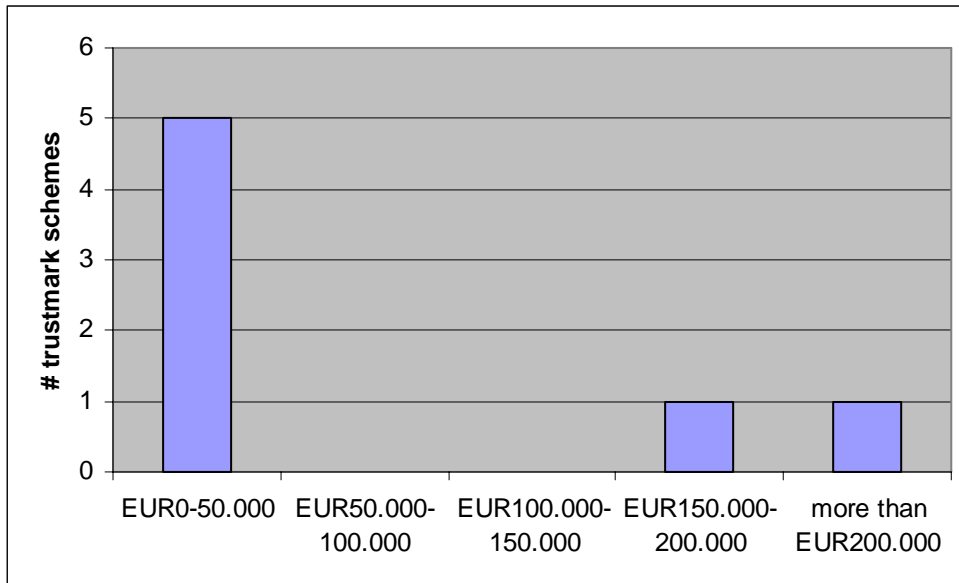
Figure 5.3.2.3
Costs break down start-up phase



§ Total revenue

The total revenue generated during the start-up phase varies per trustmark scheme. Three of the seven trustmark schemes that provided information have generated revenue during the start-up phase. The amount of revenue depends on the individual business cases and the duration of the start-up phase. An overview of the total revenue of the three trustmark schemes is presented in the figure below. Please note that the category less than EUR 50,000 includes one trustmark scheme that generated revenue, while also including four schemes that did not.

Figure 5.3.2.4
Total revenue start-up phase

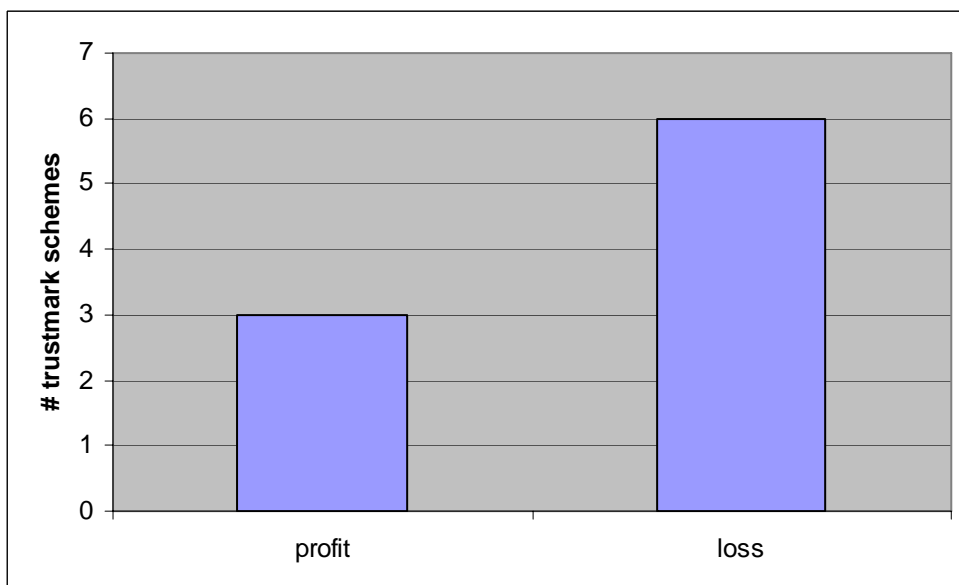


§ Revenue break down

All three trustmark schemes indicated they generated only one type of revenue during the start-up phase. One obtained project subsidy, while another obtained permanent subsidy and the third received a sponsorship. All three trustmark schemes obtained their revenue from a private source.

§ Key-performance indicators start-up phase

Figure 5.3.2.5
Profit or loss start-up phase



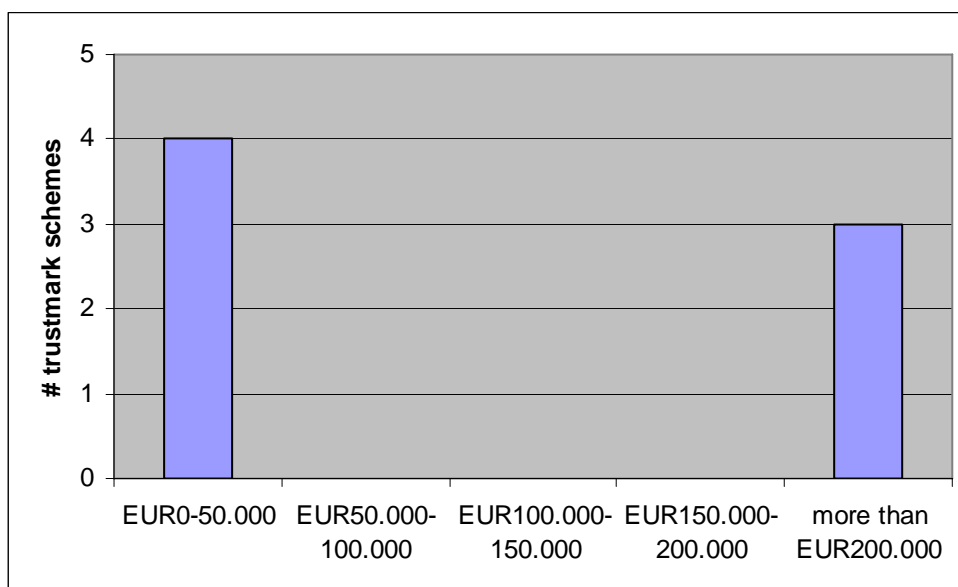
All trustmark schemes provided information on their profit or loss during the start-up phase, except for Thuiswinkel that did not distinguish a start-up phase. Three Trustmark schemes indicated they made a profit during this phase (see Figure 5.3.2.5), but no trustmark scheme was able or willing to provide their profit margin. Six of them created a loss. One of these had a loss margin of 24% and five of them had a loss margin of 100%. Only one trustmark scheme wanted to specify when they reached a break-even point, namely between 6 and 12 months.

5.3.3 Operational phase

§ Total annual costs

Seven trustmark schemes provided information on the total annual costs made during the operational phase. Of the three trustmark schemes that did not provide information, Luxembourg e-commerce certified indicated not to have reached the operational phase yet. It appears that four of these trustmark schemes have limited costs, while three of them have high operational costs. An overview of these cost is presented in the figure below.

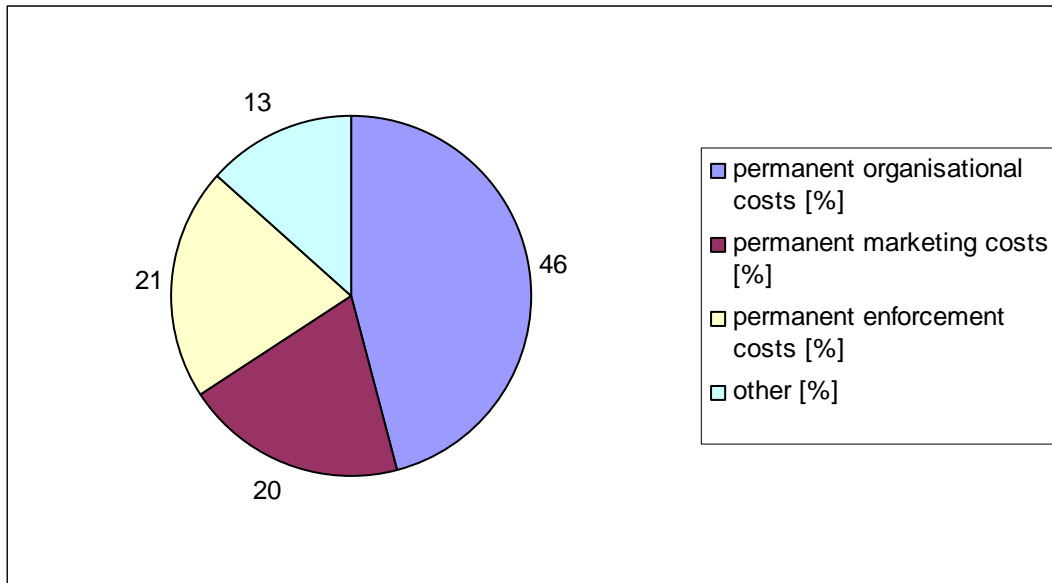
Figure 5.3.3.1
Total annual costs operational phase



§ Costs break down

The total annual costs during the operational phase as specified in the paragraph above can be broken down into several cost modules. The figure below provides a cost break down in percentages of the total costs made, based on seven trustmark schemes. As can be concluded, in general just like in the start-up phase about half of the start-up budget is spent on organisational costs. During this phase, one fifth of the budget is spent on marketing, which is a fraction more than the costs to launch a brand in the start-up phase. Also, one fifth is spent on enforcement.

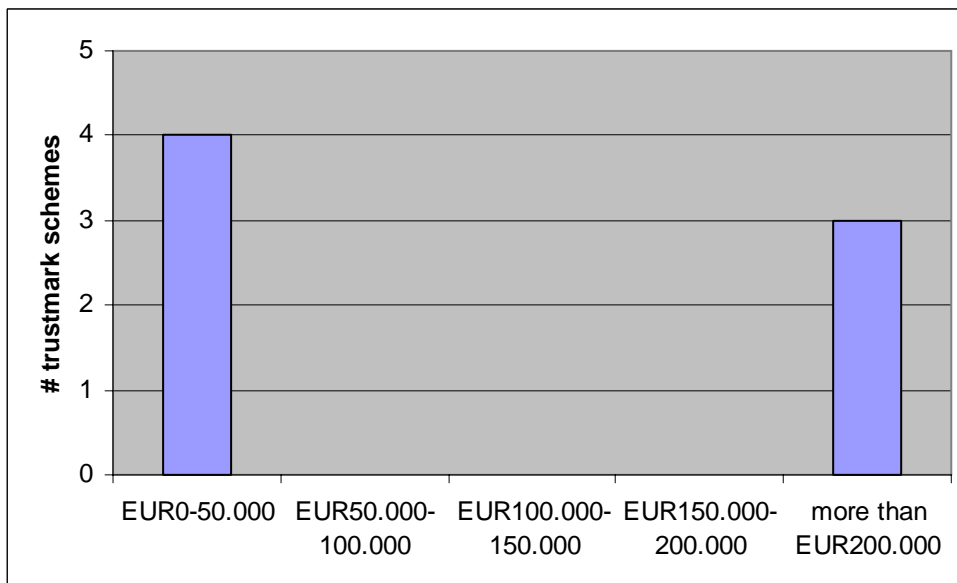
Figure 5.3.3.2
Costs break down operational phase



§ Total annual revenue

Two trustmark schemes do not manage to generate any revenue, while two others are able to generate limited revenue. In contrast, three trustmark schemes generate high revenue (see Figure 5.3.2.4). Two trustmark schemes that incur high annual costs also generate high revenue, while one does not.

Figure 5.3.3.3
Total annual revenue operational phase



§ Revenue break down

Out of seven trustmark schemes that provided information, four receive both sponsorships and user fees. One of these four also generates revenue through ‘polluter pays’, be it only 2%. Two trustmark schemes generate revenue through user fees only. One received 50% of its revenue through a project subsidy from a public source, while the other 50% came from internal means and (in this case) from a private source. Hence, an important conclusion is that in the operational phase user fees is the most significant type of revenue, followed by sponsorships. The vast majority of revenue in this phase stems from a private source.

§ Key-performance indicators operational phase

All trustmark schemes but Luxembourg e-commerce certified (because they are not operational yet) provided information on their profitability (see Figure 5.3.3.4 for a graphical overview). Five of them indicated to be profitable, while two of these five were willing to specify that their profit margin is 3% and 8%. Two trustmark schemes operate on a break-even basis. One of the respondents indicated to be able to operate at a break-even point, because the hosting organisation absorbs the organisational costs for the secretariat. Two trustmark schemes are making a loss. Their loss margins are 11% and 90%.

Of the seven respondents that indicated to operate on a break-even basis or even make a profit, four specified the period after which they had reached their break-even point. Two trustmark schemes reached their break-even point within 6 months, of which at least one managed to do so during the start-up phase (see Section 5.3.2). One trustmark scheme reached this point between 18 and 24 months and another needed more than 24 months.

Figure 5.3.3.4
Profit or loss operational phase



5.4 Critical success factors according to trustmark schemes

Contrary to all other interviewed trustmark schemes, Web Trader is no longer operational (see Section 5.3.1). The interviewee indicated that there were two important reasons for ending the scheme's operations. The costs to operate the trustmark scheme were too high. Also, they had insufficient revenue to continue. The underlying reason was that the trustmark scheme was launched to fulfil a policy goal. This goal was to create awareness with businesses and consumers and to influence behaviour i.e., introduce best practices. The trustmark was issued for free because the consumer organisations did not want to create a barrier for businesses to apply.

In addition to the questions with regard to the financial aspects, trustmark schemes were asked by means of an open question what critical success factors they could identify for setting up and running a trustmark scheme? Table 5.3.4.1 provides a top-7 of critical success factors.

Table 5.3.4.1
Top-7 critical success factors according to trustmark schemes

1. Awareness with business and consumers
2. Highly elaborated and robust code of conduct
3. Effective enforcement mechanisms
4. Number of trustmarks issued (leading to user fee revenue)
5. Trust in (independent) organisation that operates the trustmark scheme
6. Stakeholder support
7. Low up-front and operational costs

By far, most respondents mentioned that raising awareness amongst companies and consumers is a critical success factor. A highly elaborated and robust code of conduct that defines criteria exceeding the strict legal requirements and provides measurable proven legal rights increases the perceived value of the trustmark scheme. Another critical success factor is the existence of effective enforcement mechanisms, such as audits (including helping applicants to meet the criteria), monitoring and an independent alternative dispute-resolution system. The number of trustmarks issued (leading to user fee revenue) and in which pricing plays a role is critical.

Also mentioned is the trust from both businesses and consumers in the (independent) organisation that operates the trustmark scheme. A critical success factor that is closely related to this is the support of stakeholders, including government. Finally, low up-front and operational costs were indicated as critical success factor.

The respondents were also asked what they would have done differently if they could start all over again? A significant number of respondents mentioned that they felt confronted with a lack of trust in e-commerce in general, caused by the dot-com bubble burst. They had anticipated to accredit more trustmark schemes or to certify more online sellers than they have done so far.

Apart from that, several trustmark schemes indicated that they would have invested more in building business awareness of the existence of the trustmark (next to the already existing off-line brand of the organisation). Some of these respondents even state that they would

have given more focus on website owners, rather than consumers, because the demand comes from them. One respondent mentioned they would have defined more detailed security criteria and would have enforced these criteria before approval to post the trustmark on the seller's website. Another respondent said they would have started earlier by adding stronger compliance and enforcement mechanisms to the trustmark scheme. However, if this had been done too early, the stakeholders would not have accepted the scheme. Because of its current critical mass, it is now easier to introduce stronger compliance and enforcement mechanisms. Finally, one respondent would have required a user fee for using the trustmark instead of providing the service for free.

5.5 Conclusions and recommendations

§ Organisation model

A variety of organisation models exists amongst the selected trustmark schemes. *Confianza Online*, Luxembourg e-commerce certified, *Thuiswinkel* and *Trusted Shops* are stand-alone organisations. *TrustUK* is a hierarchical organisation in the sense that it accredits trustmark schemes that comply with the *TrustUK* code of practice. The *Web Trader* initiative is operated by a network of consumer organisations, each using their (different) national codes of conduct. *Euro-label* and *QWeb* have hybrid models (i.e., a combination of a hierarchy and a network). Both initiatives are based on a network of national certification bodies that co-operate under the hierarchy of *EuroCommerce* and *IQNet* (International Certification Network) respectively. *BBBOnLine* also is a hybrid organisation, namely a combination between a stand-alone (it operates as one single organisation) and a network (of their local *Better Business Bureaus* that provide the service).

All trustmark schemes but *Web Trader*, which ceased operation after 2 years, are still operational today. All initiatives have existed for 2 years or more. With 7 years of existence, *BBBOnLine* is the oldest initiative.

§ Financial model start-up phase

The start-up period of a trustmark scheme varies between 0-6 months to longer than 24 months. Some of the selected trustmark schemes have made low costs, while others have made high costs during the start-up phase. It should be stated that the amount of costs highly depends on the individual business cases and the duration of the start-up period. In general, 50% of the start-up budget is spent to get the initiative started and to create an organisation, while costs to launch a brand add up to about a quarter. 15% Of the budget is spent on the creation of a code of conduct.

The total revenue generated during the start-up phase varies per trustmark scheme. Three out of seven that provided information on this aspect indicated to have generated revenue in this phase. The generated revenue varies between EUR 0-50,000 to more than EUR 200,000. Also in this case, the amount of revenue depends on the individual business cases and the duration of the start-up period. All three trustmark schemes indicated they generated only one type of revenue during the start-up phase. One obtained a project subsidy, while the other obtained a permanent subsidy and the third received a sponsorship. All three trustmark schemes obtained their revenue from a private source.

All trustmark schemes provided information on their profit or loss during the start-up phase, except for *Thuiswinkel* that did not distinguish a start-up phase. Three trustmark schemes indicated they made a profit during this phase, but no trustmark scheme was able or willing

to provide their profit margin. Six of them generated a loss, of which one a loss margin of 24% and five a loss margin of 100%. Only one trustmark scheme wanted to specify when they reached a break-even point, namely between 6 and 12 months.

§ Financial model operational phase

Four respondents provided information on their total annual costs after becoming operational. Luxembourg e-commerce certified indicated not to have reached the operational phase yet. Four trustmark schemes have limited costs (EUR 0-50,000), while three have high operational costs (more than EUR 200,000). In general just like in the start-up phase about half of the start-up budget is spent on organisational costs. During this phase, one fifth of the budget is spent on marketing, which is a fraction more than it costs to launch a brand in the start-up phase. Also, one fifth is spent on enforcement.

Two trustmark schemes do not manage to generate any revenue, while two others are able to generate limited revenue (EUR 0-50,000). In contrast, three trustmark schemes generate high revenue (more than EUR 200,000). Two trustmark schemes that have high annual costs also generate high revenue. One does not. Out of seven trustmark schemes that provided information, four receive both sponsorships and user fees. One of these four also generates revenue through 'polluter pays', be it only 2%. Two trustmark schemes generate revenue through user fees only. One received 50% of their revenue through a project subsidy from a public source, while the other 50% came from internal means and (in this case) from a private source. The vast majority of revenue in this phase stems from a private source. Hence, an important conclusion is that in the operational phase user fees is the most significant type of revenue, followed by sponsorships. The generation of revenue through user fees (in addition to sponsorships) may therefore even be a critical success factor.

All trustmark schemes but Luxembourg e-commerce certified (because they are not operational yet) provided information on their profitability. Five indicated to be profitable, while two of them were willing to specify that their profit margin is 3% and 8%. Two trustmark schemes operate on a break-even basis. One of the respondents indicated to be able to operate at a break-even point, because the hosting organisation absorbs the organisational costs for the secretariat. Two trustmark schemes are making a loss. Their loss margins are 11% and 90%. Hence, the vast majority of the selected trustmark schemes are profitable or operate on a break-even basis.

Of the seven respondents that indicated to operate on a break-even basis or even make a profit, four specified the period after which they had reached their break-even point. two trustmark schemes reached their break-even point within 6 months, of which at least one managed to do so during the start-up phase. One trustmark scheme reached this point between 18 and 24 months and one needed more than 24 months. Hence, at least three trustmark schemes managed to reach their the break-even point at a reasonable point in time (less than 2 years).

Given the analysis above, one can argue whether trustmark schemes that obtain sponsorships are truly commercially viable. This actually depends on the nature of the sponsorships i.e., their source and whether they are incidental or structural. From an economic perspective, the trustmark scheme that operates on a break-even basis because the secretarial costs are absorbed by the hosting organisation is not commercially viable by itself. However, due to this structural sponsorship this trustmark scheme is able to sustain its operations. Fact is, however, that at least three and a maximum of six of the assessed trustmark schemes manage to operate with a profit or at a break-even point in the end and to

reach their break-even point at a reasonable point in time. Hence, it can be concluded that at least three and a maximum of six of these trustmark schemes are commercially viable.

§ Relation between organisation model and financial model

Annex 4 includes an overview of the selected trustmark schemes' organisation model and their organisation profile. There is no correlation between the type of organisation model (stand-alone, hierarchical or network) and commercial viability. Whether a trustmark scheme is provided by a new or an existing (online) brand does not have any effect on its commercial viability. Also, no correlation can be found with commercial viability and relevant elements of the organisation profile, such as target audience and (third-party) dispute settlement. However, organisations that provide the trustmark scheme as their only service have a negative correlation with commercial viability. Hence, the provision of a larger service portfolio next to the trustmark scheme itself is a critical success factor.

§ Critical success factors according to trustmark schemes

The following top-7 list of critical success factors were identified based on the information provided by the selected trustmark schemes:

1. Awareness with business and consumers;
2. Highly elaborated and robust code of conduct;
3. Effective enforcement mechanisms;
4. Number of trustmarks issued (leading to user-fee revenue);
5. Trust in (independent) organisation that operates the trustmark scheme;
6. Stakeholder support;
7. Low up-front and operational costs.

Interesting to note is that some of the respondents stated that if they could start all over again, they would have given more focus on creating awareness with website owners, rather than consumers, because the demand comes from them.

With regard to enforcement, one respondent remarked that they would have started earlier by adding stronger compliance and enforcement mechanisms to the trustmark scheme. However, if this had been done too early, the stakeholders would not have accepted the scheme. Because of its current critical mass, it is now easier to introduce stronger compliance and enforcement mechanisms.

§ Recommendations on commercial viability of trustmark schemes

As concluded earlier, all three trustmark schemes that provided information on their revenue generated during the start-up phase obtained their revenue from a private source. Also in the operational phase, the vast majority of revenue stems from a private source. At least three and a maximum of six of the selected trustmark schemes have proven to be commercially viable. Therefore, it is not recommended to financially support trustmark-scheme organisations in their operations with public means.

However, when looking at the critical success factors indicated by the trustmark schemes themselves, the creation of awareness could contribute to their commercial viability. It is recommended to allocate public means to awareness raising activities, while more emphasis could be given on businesses rather than consumers. Ideally, the business and consumer organisations play a leading role in this. Project subsidies can be awarded to organisations that enrol awareness raising activities, such as organising workshops, website, newsletters,

articles in members' magazine, free-press, awareness questionnaires, or (online) awareness campaigns.

For any new trustmark scheme, it is recommended to subsidise the creation of a code of conduct (15% of start-up costs) through public means. This does not only lead to a cost reduction in the start-up phase, but also shortens the start-up period. This may be done by directly subsidising the creation of a code, for example via a project subsidy. Alternatively, public means could be used to allocate experts who provide assistance or guidance in the creation of the code of conduct.

6 Overall conclusions and recommendations

This chapter discusses the overall conclusions of the project. It identifies converging and diverging issues resulting from the previous analyses. As such, it synthesises the business and consumer perspectives, the legal analysis and the commercial viability analysis. Based on this synthesis, additional conclusions and recommendations are formulated.

6.1 Elaboration of the trustmark scheme

While consumers feel that their involvement in the elaboration and conception of the trustmark scheme is very important, businesses consider that this is in the first place up to them. From a legal point of view, the legitimate character of a trustmark scheme is determined by a number of factors, amongst others the intervention of both business and consumers. Normative sources, however, stress and favour the active intervention of consumers.

Considering that most of the benchmarked trustmark schemes are not elaborated in close consultation and co-operation with consumers, we recommend that their active involvement, for example via the relevant consumer associations, is encouraged.

6.2 Public endorsement – public support.

In addition, attention must be paid to the fact that consumers find it important that a trustmark scheme is endorsed or supported by public authorities. Ironically, public support or endorsement does not necessarily guarantee a high level of quality. Therefore, we recommend that European standards or some minimum set of quality criteria are defined. This could for example be done through a Commission Recommendation or other regulatory instrument.

The adoption of such a European minimum standard can also be advocated by the conclusion that trustmark schemes score differently and insufficiently on several criteria. This conclusion remains valid with metalabels or overarching trustmark schemes. They do not prevent independent schemes from providing different levels of trust, e.g. they score differently on the same criteria.

Therefore, we recommend that overarching trustmark schemes should define common requirements, common structures and common core principles, which can be tailored to specific local needs, for participating trustmark schemes.

6.3 Order procedure

Both consumers and businesses find it very important to know when one is legally bound to an agreement, e.g., purchase order. Most Codes of Conduct recognize the importance of this. The problem, however, lies within the difficult articulation between the Directive on electronic commerce and the Directive on distance contracts. Some Codes of Conduct contemplate the positive law obligations very well and demonstrate their added value by describing in a clear, easy to understand and transparent manner how an order procedure works. Furthermore, most error-detection mechanisms are directed at technical errors. These safeguards should also encompass errors in consent.

It can be recommended that trust mark schemes adopt as a best practice the rule that consumers are only bound provided they have accepted the offer after having received and reviewed a written confirmation of their order, e.g., sent via electronic mail.

6.4 Complaints procedure, Dispute Resolution and Enforcement

Both consumers and businesses find it very important that there is a comprehensive Code of Conduct and an effective enforcement infrastructure, including a complaints procedure and alternative dispute resolution. In contrast, it is demonstrated that the average evaluation related hereto is negative and that almost none of the benchmarked trustmark schemes have a full-scale enforcement structure in place.

One of the reasons for this can be related to the costs of such a mechanism (21%). The commercial viability analysis (see Chapter 5) shows that trustmark schemes prefer in the start-up phase quantity (number of merchant members) over quality (effective enforcement infrastructure).

In this regard, overarching structures or a European enforcement mechanism could contemplate the complaint handling and dispute resolution of single trustmark schemes. Not only would one profit from the economies of scale, but this 'pan'-European structure would also be a true independent alternative dispute-resolution body. Such an infrastructure could also be linked to the existing EEJ-Net.

6.5 Applicable law

In line with Article 3 of the electronic commerce Directive, information society service providers are only subject to the law of the Country of Origin (place of establishment). However, the Directive and Private International law include derogations of the Country of Origin principle and in principle consumers cannot be deprived of the protection offered by their national law. Although this is a very complex field of law, we recommend that these two principles are reconciled as much as possible.

Almost all trustmark schemes and Codes of Conduct only refer to the law of the Country of Origin as applicable. Most trustmark schemes and Codes of Conduct do not indicate that consumers cannot be deprived of the protection offered by their national law. Therefore, we recommend that trustmark schemes and Codes of Conduct inform consumers that their national law can be important. In this view, further harmonisation of consumer protection legislation can be advocated.

6.6 The user fee dilemma

As concluded in the business and consumer analysis (see Section 3.3.3), most business representatives indicated they prefer the trustmark scheme service to be free of charge or to be provided at a low fee. On the other hand, trustmark schemes very much rely on user fees for their commercial operations (see Section 5.5). The consequences of this so-called 'user fee dilemma' are limited. Most of the assessed trustmark schemes prove to be commercially viable because they also are able to generate sponsorship revenue from a private source. Therefore, there seems to be no need from a government perspective to intervene in this market-driven pricing mechanism. The table below provides an overview of the overall conclusions and recommendations.

Table 6.6
Overall conclusions and recommendations

	Consumers	Business	Legal Criteria	Commercial	Recommendation
Elaboration	Involvement is important Consumers believe that public endorsement is important	Involvement is important	Legitimacy (64.44%) is determined by a number of factors, notably consumer involvement and public endorsement	Not applicable	Active intervention of all the different stakeholders, notably consumer and business associations Set EU minimum standard for trustmark scheme quality
Order procedure	Very important	Very important	Confirmation process (68.89%)	Not applicable	Added value of Codes: - Clear, easy to understand and transparent manner information. - Error detection also in relation to consent errors.
Applicable law	Law of residence	Law of place of establishment	Applicable law (53.33%)	Not applicable	Reconcile: - Country of Origin principle - Consumer protection legislation.
Dispute resolution and enforcement	Very important	Very important	Pro-active monitoring (40.71%) Monitoring (49.44%) Enforcement (39.29%)	High enforcement costs (21% of operational budget)	Co-operation between schemes or outsourcing to pan-European structure (EEJ Net).
User fee dilemma	Not applicable	Low user fees or free of charge	Not applicable	High user fees	No government intervention required.

ANALYSIS AND DEFINITION OF COMMON CHARACTERISTICS OF TRUSTMARKS AND WEB SEALS IN THE EUROPEAN UNION

ANNEXES

Authors:	Dr. Ronald de Bruin (ECP.NL), Ewout Keuleers (CRID), Christophe Lazaro (CRID), Prof. Yves Pouillet (CRID) and Marjolein Viersma (ECP.NL)
Version:	Final version 2.4
Date:	15 March 2005
Contract no:	B5-1000/03/000381

Table of content

1	LIST OF SELECTED TRUSTMARK SCHEMES (DELIVERABLE WP1).....	4
2	BENCHMARK CRITERIA (DELIVERABLE WP2).....	5
	EXECUTIVE SUMMARY	5
	1. SCOPE OF THE QUALITY ANALYSIS: A GLOBAL APPROACH.....	7
	2. THE NORMATIVE SOURCES.....	9
	2.1 Sources of self-regulation or soft law	9
	2.2. Sources of EU law or hard law	14
	3. QUALITY ASSESSMENT OF TRUSTMARK SCHEMES: SELECTION OF CRITERIA	21
	3.1. List of general criteria	21
	3.2. A pragmatic approach: the life cycle of the scheme	22
	3.3. “Must-have” vs. “Nice-to-have” criteria	24
	3.4. Selection of and comments on benchmarking criteria	26
	1. ELABORATION OF THE TRUSTMARK SCHEME	27
	1.1 Legitimacy of the scheme	27
	1.2. Code of conduct.....	27
	1.3 Security.....	29
	2. INFORMATION ON THE TRUSTMARK SCHEME.....	32
	2.1 Identification of the trustmark scheme provider	32
	2.2. General information on the trustmark scheme’s functioning.....	33
	3. PARTICIPATION IN THE TRUSTMARK SCHEME.....	37
	3.1. Accessibility of the trustmark scheme.....	37
	3.2. Procedure of assessment.....	38
	3.3. Mutual recognition with other trustmark schemes.....	40
	4.CODE OF CONDUCT	41
	4.1. General principles.....	41
	4.2. Information on merchant.....	46
	4.3. Information on products and services.....	48
	4.4. Conclusion of the contract	53
	4.5. Customer service.....	63
	4.6. Commercial communications and fair marketing practices.....	68
	4.7. Security of system and payment.....	72
	4.8. Personal-data protection.....	75
	4.9. Protection of children	77
	5. PROACTIVE MONITORING	81
	5.1.Monitoring mechanisms.....	81
	5.2. Monitoring reports.....	82
	6. COMPLAINT PROCEDURE.....	83
	6.1. Accessibility and convenience	83
	6.2. Quality of the complaint procedure	83
	6.3. Alternative dispute resolution.....	84
	7. ENFORCEMENT SYSTEM.....	86
	7.1 Quality of the enforcement process	86
	8. RELATIONSHIPS WITH PROTAGONISTS	89
	8.1. General relationships.....	89
	8.2. Relationship with consumers	90
	8.3. Relationship with businesses.....	91
	4. CONCLUSIONS AND FINAL REMARKS	92

3	RELEVANT EU REGULATORY SOURCES (DELIVERABLE WP2)	93
4	BUSINESS MODELS ANALYSIS (DELIVERABLE WP3)	97
5	TRUSTMARK SCHEME QUESTIONNAIRE (DELIVERABLE WP3)	99
6	CONSUMER QUESTIONNAIRE (DELIVERABLE WP4)	105
7	BUSINESS QUESTIONNAIRE (DELIVERABLE WP5)	109

1 List of selected trustmark schemes (deliverable WP1)

BBBOnLine	Steve Cole and Charlie Underhill (CBBB)
Confianza Online	Javier Conzalez
Euro-label	Thorsten Scharmacher
Luxembourg e-commerce certified	Dominique Ferrand (Centre de Recherche Public Henri Tudor)
Thuiswinkel	Wijnand Jongen
Trusted shops	Thomas Karst
TrustUK	Robert Dirskovski (DMA)
Web Trader	Machiel van der Velde (Consumentenbond)
WebTrust	Han Boer (KPMG) and Jan Pasmooij (NIVRA)
QWeb	Dario Agalbato (IGQ)

2 Benchmark criteria (deliverable WP2)

Executive summary

In this paper we will present the Projects' methodology in relation to the selection of legal benchmark criteria and the evaluation of these criteria. We stress that a multitude of criteria can be identified to assess the legal quality of a trustmark scheme. Even though codes of conduct are the core of most self-regulatory models, we hold that the quality of the trustmark scheme also depends on other criteria such as notably complaint handling, organisation and other scheme properties. In this regard, we underline that we adopt an open and **functional definition** of the concept of **codes of conduct**, *i.e.*, any document containing trustmark scheme obligations, principles or norms, this irrespective of their location on the website or formal label.

In order to avoid a too narrow basis of quality assessment, we advocate a more **global approach**, encompassing a number of criteria derived from various sources of normative instruments.

From these different normative sources, including dispositions of hard and soft law, the highest common factors or criteria were identified. This comparative process resulted in the elaboration of a list of more than 40 general selection criteria¹.

Afterwards, this general list was converted into a more functional synopsis. For the purpose of the phases of the "**life cycle**" of a trustmark scheme, *i.e.*, from conception, dissemination to enforcement, different criteria were grouped and ordered in a more pragmatic and systematic manner.

Eventually, a "short list" of criteria was used to identify a number of legal criteria a scheme should have to distinguish itself. These so-called "**must-have**" criteria have been chosen due to their legal added value. In contrast to the remaining list of "*nice-to-have*" criteria, the list of 15 "**must-have**" criteria allows to have a better general understanding of the legal quality of a trustmark scheme and their respective positions in relation to the other schemes.

Each of the criteria, both "must-have" and "nice-to-have" shall be evaluated according to a two-phased procedure:

- Phase 1: **vertical evaluation** of each trustmark scheme with comments on each criterion;
- Phase 2: **horizontal evaluation** of the trustmark schemes assessed in the first phase. During this phase and in view of the comments made, a value on a scale of five will be given to each criterion².

Once the evaluation is done, conclusions will be formulated in view of the trustmark scheme or/and criteria.

Finally, it is important to emphasize the following elements.

- The evaluation is an "**on sight desk evaluation**"³: We only consider information that is publicly available on the trustmark scheme website. To stimulate consumer confidence,

¹ See *infra* 3.4. Selection and comments of benchmarking criteria,

² Whereas five reflects the maximum value.

³ The evaluation takes into account the information published or publicly available at the 1st of November 2004.

we hold that it is of paramount importance that the public, including consumers, receive comprehensive and transparent information on the scheme's functioning and characteristics. For this reason it is important that consumers see - and are allowed to verify – the functioning of a trustmark scheme concerned. What they do not know, they cannot verify, nor can it stimulate their confidence. In other words, what happens in the scheme's internal "black box" does not stimulate confidence. Therefore, back office information that is made available on request, e.g., the over 300 pages code of conduct of Webtrust Netherlands, is excluded from the scope of evaluation.

- § The **evaluation focuses on the "second-level applications" of complex models** (hierarchical and hybrid models). A variety of organisation models exists among the selected trustmark schemes. Besides classical *stand alone* models, a certain number of models are characterised by their structural complexity. Some of them are based on a *hierarchical* structure⁴, others on a *network* structure⁵ and finally some on a *hybrid* structure (*i.e.*, a combination of a hierarchy and a network)⁶.

The existence of complex models – especially those constituted by different levels (hierarchical or hybrid structures) – raised some methodological difficulties as to the choice of the structural level that would be the subject of the evaluation. In order to make a meaningful comparative evaluation, it was decided to focus mainly on the concrete applications (lower second level) of the complex models⁷. For this reason, all the trustmark schemes could be benchmarked at the same level, *i.e.*, the one with the most direct impact on subscribers and consumers.

In this context, *Labelsite* – the French application of the hierarchical organisation Euro-Label – and *SafeBuy* – one of the schemes accredited by TrustUK – were selected⁸.

- The **evaluation is made at a certain time** (time stamped). For this reason, we cannot guarantee that providers of 'trusted services' have not modified their trustmark scheme. We noticed that during the short time lapse between the vertical evaluation and the horizontal one, some schemes had already been modified. So we might not exclude that our assertions will be still valuable at the moment these study's results are published. The fact that the information is modified frequently pleads for the obligation of each Trustmark to time stamp each version and to archive the previous versions in case of litigation arising from the different versions existing at the precise moment of the labelled transaction.
- § This benchmarking activity implies to a certain extent a **subjective aspect** regarding the selection of criteria⁹ and the proper evaluation of each criteria.

⁴ An organisation accredits trustmark schemes that comply with the "hierarchical" code.

⁵ A network is composed by (consumer)organisations, each using their (different) national code.

⁶ A network of certification bodies, cooperating under the hierarchy of a particular organisation.

⁷ The higher level of scheme was therefore not benchmarked.

⁸ Nevertheless, considering the high number of low level applications of the Qweb scheme (22 certification bodies, including 12 in Italy), the evaluation was conducted from the higher level of this hybrid scheme instead of picking a certification body at random.

⁹ As to the identification of criteria, one has to bear in mind that most of the attributes of a trustmark scheme can be considered part of a complex network of relationships. Therefore, the same attribute can be viewed from various perspectives.

1. Scope of the quality analysis: a global approach

Trustmarks or seals of approval are currently one of the chief mechanisms for promoting consumer confidence in electronic commerce. Different types of organisations (usually referred as code owners) establish standards (codes of conduct) for conducting e-commerce and certify that particular online businesses (code subscribers) have met those standards. In other words, in order to be certified with a trustmark, a provider of information society services¹⁰ has to comply with the code of conduct of the trustmark organisation. The provisions of the code of conduct state how the subscriber must conduct his business and should improve consumer confidence.

In this regard, we cannot deny that the code of conduct is the central element of such schemes. This paramount characteristic of codes of conduct is the reason why most surveys on trustmark schemes generally focus on this sole aspect. The examination of the content of the code of conduct allows assessing the level of the requirements imposed on the subscribers. Therefore, it allows to a certain extent the evaluation of the quality of a trustmark scheme. Here the code almost plays the role of a mirror that reflects the quality of the trustmark scheme.

For instance, in a survey conducted within the framework of the 17th BILETA Annual Conference, the authors compared the certification process and performance of nine different trustmark schemes¹¹. More particularly, they assessed the *content* of the codes of conduct of the selected schemes according to six macrocriteria that, in their view¹², represent the main problematic issues regarding B2C e-commerce:

1. Identity of the vendor;
2. Products and services;
3. Order procedures;
4. Customer service;
5. Reference to legislation;
6. Security.

In our opinion, such an approach is not sufficient to get a global overview of the quality a trustmark scheme. The latter is indeed determined by a complex range of different factors. This global approach is based upon a profound reading of the different normative instruments regarding trustmark schemes¹³. These normative sources all aim to provide recommendations on the overall organisation and proper functioning of trustmark schemes as such. Since they are not limited to the content of the code of conduct, these recommendations constitute a broader, all encompassing basis for good online practices.

An eloquent illustration of such a global approach are the European Trustmark Requirements elaborated within the framework of the e-confidence initiative. In addition to the requirements

¹⁰ As defined by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998.

¹¹ F. NORDQUIST, F. ANDERSSON and E. N. DZEPINA, "Trusting the Trustmark?", 17th BILETA Annual Conference, April 5th-6th, 2002, Free University Amsterdam, p. 4, available on line at <http://www.bileta.ac.uk/02papers/nordquist.html>.

¹² In fact, their selection of criteria is based on a study of Consumer International that raises a number of issues in regard of the lack of e-vendors compliance with existing consumer protection law. See, Consumer International, "Should I buy? Shopping online 2001: an international comparative study of electronic commerce". <http://www.consumersinternational.org>.

¹³ See, *infra*, Chapter 2: The normative sources.

related to the content of the code of conduct, the European Trustmark Requirements address the following issues:

1. Transparency of consumer and business trustmark schemes;
2. Accessibility and visibility of consumer and business trustmark schemes;
3. Operation of trustmark schemes;
4. Assessment of trustmark scheme applicants;
5. Monitoring system;
6. Enforcement system;
7. Technical security.

As demonstrated in this document, the content of the code is one of the relevant factors to benchmark the quality of a trustmark scheme, but not the only one. In this context, we have to take into account in our benchmark list a large range of factors concerning, on the one hand, the content of the code and, on the other hand, the other aspects of the organisation and functioning of a trustmark scheme.

In order to develop a model of trust that describes what legal factors affect the quality of a trustmark scheme, we do not therefore limit our analysis to a single benchmarking of the content of the selected trustmark schemes' codes of conduct. We go further in adopting a more global perspective and covering the main aspects of this type of service.

2. The normative sources

In this chapter, we present a part of the normative sources we will refer to for the legal analysis. From a methodological point of view, those sources constitute the framework that will help us to develop the list of relevant criteria in order to benchmark the selected trustmark schemes.

We decided not to divide the benchmarking in different parts, based on different regulation instruments (self-regulation sources and EU sources) for the following reasons:

- The main objective of the project is to formulate conclusions on the usefulness of trustmarks and the conditions under which trustmarks would gain more acceptance from consumers and businesses with a view to improve e-commerce confidence. From this perspective, it will be more practical to benchmark the different trustmark schemes from a uniform, single base;
- From a methodological point of view, this single base of benchmarking will allow us to avoid overlapping and coherence problems and therefore to draw clear conclusions as to the state of the art of trustmark programs;
- However, we will indicate for each criterion of the benchmark list the different regulation instruments we refer to¹⁴;

Nevertheless, at this stage, we do not analyse in detail the content of those instruments, but rather provide a global overview of their provisions¹⁵.

2.1 Sources of self-regulation or soft law

At European level, the importance of building consumer confidence on the internet has been considered by the European Union in its eEurope Action Plan. In a Communication dedicated to this eEurope project, under the section entitled “*accelerating e-commerce*”, the EU indicates what the Commission considers a flexible regulatory approach¹⁶. The Commission states that “*more emphasis must therefore be placed on the role of self-regulation and co-regulation, especially in helping to build consumer confidence*”.

It underlines the role of market-based mechanisms in order to promote consumer confidence and trust; those mechanisms are needed to complement the existing regulation, to pull down existing impediments to B2B and B2C e-commerce transactions. Within these mechanisms, trustmarks (or trust seals) and associated codes of conduct and alternative dispute resolution have to be considered.

In May 2000 the Commission launched the eConfidence initiative. This initiative is presented as “*a common package of measures, which include as its main components the promotion of high standards of good business practices (e.g. codes of conduct, trust marks, complaint settlement procedures), as well as easy and affordable access to third-party alternative dispute resolution (ADR) systems, in particular for settling disputes arising from the expected increase in cross-border transactions over the Internet*”¹⁷.

¹⁴ Cf., Benchmark criteria; WP 2: List of relevant criteria and regulations.

¹⁵ A more profound analysis will be provided in the chapter dedicated to the presentation of the criteria included in the benchmark list, see *infra*.

¹⁶ eEurope, An Information Society For All, Communication on a Commission initiative for the Special European Council of Lisbon, 23 and 24 March 2000. See also the recent eEurope 2005 Action Plan, http://europa.eu.int/information_society/eeurope/2005/index_en.htm.

¹⁷ Within this framework, an on-line “eConfidence Forum” has been set up, mainly to connect different initiatives worldwide, and to provide a completely open platform for exchange and dialogue between interested parties. See <http://econfidence.jrc.it>.

Within this framework, different documents were drafted and published. In the context of our analysis we especially refer to two documents directly linked to trustmark and code of conduct issues:

- The European Trustmark Requirements (or ETR);
- The second draft principles for e-commerce codes of conduct.

At international level, we also take into account the proceeds of the Global Business Dialogue on e-commerce (GBDe), one of the world's leading private sector voices on e-commerce policy¹⁸. For the last 6 years, this organisation - in consultation with governments and other international organisations – has tried to identify solutions and to provide input on regulation or business self-regulatory codes of conduct. The GBDe created a specific working group dedicated to “Consumer Confidence”. Under this broad umbrella, it proposes the use of trustmark schemes to encourage good e-business practices by merchants and to help consumers to identify reliable merchants.

Those three “soft-law” instruments represent the keystone of our legal analysis. They guided us in the drafting of a list of criteria that will be used to benchmark the selected trustmark schemes¹⁹.

The elaboration of such a benchmark list on the basis of those instruments was a sensitive task. In this respect, we followed a three-step approach:

- Deciphering phase: to begin with, we had to decipher their contents because their requirements are sometimes expressed in an ambiguous manner;
- Comparison phase: subsequently, we had to compare all those instruments in order to emphasise the common and divergent characteristics;
- Identification phase: finally, we had to select the most substantial requirements in order to include them into the benchmark list²⁰.

2.1.1. European Trustmark Requirements (ETR)

a) *Origin and scope*

In the framework of the EU ‘eConfidence initiative’, the European business confederation UNICE²¹ and the Bureau Européen des Unions de Consommateurs (BEUC), also known as the European Consumers organisation²², agreed on a common proposal for a European framework for e-commerce trustmark schemes, called the *eConfidence Project*. This project includes the European Trustmark Requirements (hereafter ETR)²³ and is complemented by a detailed system for approval and monitoring based on assessment by an independent third party.

This document, as underlined in its preamble, aims to provide a high standard of consumer protection in electronic commerce and encourages the sale of goods and services on the

¹⁸ <http://www.gbde.org>.

¹⁹ See the list of criteria and relevant regulations, *infra*.

²⁰ See also *infra* on the list of general criteria (3.1), the list of criteria according to the life cycle of a trustmark scheme (3.2) and the list of “*must-have*” criteria (3.3).

²¹ Union of Industrial and Employers’ Confederations of Europe (UNICE), <http://www.unice.org>.

²² Bureau Européen des Unions de Consommateurs (BEUC), <http://www.beuc.org>.

²³ UNICE-BEUC eConfidence Project, 22 October 2001, <http://www.euractiv.com/ndbtext/infosoc/econfidence.rtf>.

Internet. The requirements are aimed at general trustmarks for e-commerce directed towards consumers (B2C).

In this context, the trustmark schemes are encouraged to meet or exceed the ETR. Trustmark schemes that meet the ETR may voluntarily decide to participate in the European e-confidence initiative. Under this initiative trustmark schemes that meet the ETR can increase their visibility at European level.

b) Content of the requirements

The ETR address the following issues:

1. High standards, measurability and purpose of trustmark schemes;
2. Transparency of consumer and business trustmark schemes;
3. Accessibility and visibility of consumer and business trustmark schemes ;
4. Scope and content of trustmark schemes:
 - Language
 - Commercial communications and fair marketing practices
 - Children
 - Pre-contractual information
 - § *General*
 - § *Information on the goods and services on offer, including price*
 - § *Information on the contract (terms and conditions)*
 - § *Supplementary to all legally required information and other relevant information the subscriber must provide*
 - Confirmation process
 - Contractual performance
 - § *Acknowledgement of order*
 - Payment
 - Security
 - § *Security of system*
 - § *Security of payment*
 - Data protection
 - Internal complaint management and dispute settlement for consumer complaints;
5. Operation of trustmark schemes;
6. Assessment of trustmark scheme applicants;
7. Monitoring system;
8. Enforcement system;
9. Technical security.

2.1.2 E-Confidence Initiative Working Documents

a) *Origin and scope*

Within the framework of the eConfidence initiative, a working group has published a set of principles for e-commerce codes of conduct and trustmark schemes. In this regard, we especially refer to the second draft of principles, published in March 2001²⁴.

This set of documents includes:

- General principles for generic codes of practice for the sale of goods and services to consumers on the Internet;
- Specific guidelines for the interpretation of the general principles;
- Guiding principles for 'approval and monitoring' bodies;
- Options for 'Approval and Monitoring'.

b) *Content of the principles*

In our analysis, we mainly focus on the first two documents.

“General principles for generic codes of practice for the sale of goods and services to consumers on the Internet”

1. Fairness and equity;
2. Added value;
3. Transparency;
4. Openness and non-discrimination;
5. Global Dimension;
6. Social responsibility;
7. Compliance;
8. Complaint handling and dispute resolution;
9. Security;
10. Data protection.

“Specific guidelines for the interpretation of the general principles”

1. Commercial communications
 - 1.1. General
 - 1.2. Use of technology
 - 1.3. Children
2. Actions to be taken before the conclusion of the contract
 - 2.1. General
 - 2.2. Information on the goods and services on offer, including price
 - 2.3. Information on the contract and contractual obligations, terms and conditions
 - 2.4. Consent of children to contract
 - 2.5. Confirmation process by consumers
3. Contractual performance
 - 3.1. General
 - 3.2. Business acknowledgement
 - 3.3. Payment
4. Security
5. Data protection

²⁴ Those principles are available on the 'eConfidence Forum' website, <http://econfidence.jrc.it>.

6. Complaint handling and dispute settlement
 - 6.1. Complaint handling
 - 6.2. Dispute settlement
7. Compliance
 - 7.1. Monitoring
 - 7.2. Remedies/Sanctions
 - 7.3. Code owners trustmarks

2.1.3 Global Business Dialogue on e-commerce Recommendations

The third self-regulatory source we refer to is the “Recommendations for Trustmarks”²⁵ developed by the Global Business Dialogue on e-commerce during its 2001 Conference in Tokyo (GBDe).

As stated in the introduction of this document, *“the GBDe endorses the use of trustmark programs in order to encourage good online business practices by merchants and to assist consumers in identifying merchants they can trust. To help avoid confusion for consumers among different trustmark programs offering different levels of protection, the GBDe has thus developed guidelines, to help ensure greater transparency, minimum voluntary standards and comparable levels of protection among competing trustmark programs (...)”*²⁶.

In this document, the GBDe particularly insists on the following requirements, considered crucial for the development of trustmark programs:

- affordable, in particular to SMEs;
- rigorous enforcement, by providing clear monitoring and reporting mechanisms and guaranteeing neutrality of their enforcement decisions;
- the websites of service providers or merchants should be easy to access and made well-known to the public;
- development in consultation with all stakeholders;
- use of appropriate security measures to prevent misuse of the trustmark;
- offer a mechanism for consumer redress (along the lines of the GBDe ADR recommendations);
- minimum standards of behaviour by merchants in the areas of online business practices, privacy protection and complaints handling, (in line with GBDe recommendations) should be required.

These recommendations are divided into two sections. The first sets out general guidelines for companies or organisations that develop trustmark programs (“Guidelines for certifiers”). The second sets out general guidelines for merchants who establish best business practices governing commercial relations between merchants and consumers that should be required by trustmark programs (“Guidelines for merchants”).

Moreover, this document also includes Recommendations to public bodies relating to the development and promotion of such programs.

²⁵ See the so called “Tokyo Recommendations” (Consumer confidence: Trustmarks), GBDe Conference, 13 and 14 September, 2001, Tokyo, Japan, <http://www.gbde.org/acrobat/trustmarks01.pdf>.

²⁶ GBDe adds in this document that these guidelines will be developed further in response to comments received from business and consumer groups.

b) Content of the Guidelines

“Guidelines for certifiers”

1. Accessibility;
2. Enforcement mechanism;
3. Visibility;
4. Stakeholders participation;
5. Security;
6. Redress;
7. Flexibility and mutual recognition.

“Guidelines for merchants”

1. Accuracy and accessibility of information;
2. Marketing practices;
3. Information about the merchant;
4. Information about the goods and services;
5. Information about the transaction;
6. Cancellation/Return/Refund policies;
7. Security;
8. Customer service and/or support;
9. Warranty;
10. Privacy;
11. Unsolicited e-mail;
12. Dispute resolution.

2.2. Sources of EU law or hard law

2.2.1. EU regulations and trustmark schemes

From a general point of view, we can observe that most EU normative sources do not directly address or regulate trustmark scheme issues. We should of course not be surprised that there is no specific legal framework in that field. This characteristic corresponds indeed to a policy-making process or governance, peculiar to the European construction.

As stated in its White paper on European Governance, “*legislation is often only part of a broader solution combining formal rules with other non-binding tools such as recommendations, guidelines, or even self-regulation within a commonly agreed framework*”²⁷.

Nevertheless, some EU instruments state explicit reference to “codes of conduct”. In this section, we will therefore pay particular attention to some EU instruments regarding commercial practices, notably distance selling, electronic commerce and unfair commercial practices²⁸, since they

²⁷ See White paper on European Governance, COM (2001) 428 final, http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0428en01.pdf

²⁸ In other fields, see article 27, § 1 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.*, n° L 281, 23-11-1995, p. 31. It encourages the drawing up of codes of conduct intended to contribute, depending on the specific nature of the sectors concerned, to the correct application of national provisions. The editors of such codes could submit them to monitoring authorities who would verify their conformity with existing regulations. See also the European Council Recommendation 98/560/CE of 24 September 1998 about the development of the competition within the audiovisual and information services by promoting the protection of minors and human dignity, *O.J.*, L 270,

provide some valuable information about the role that a code of conduct could play within a trustmark scheme²⁹.

a) The Recommendation on distance selling

The Commission Recommendation of 7 April 1992 on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling) is perhaps the exception that proves the rule. As indicated by its title, this EU Recommendation is entirely dedicated to codes of conduct³⁰.

Due to the specific risks introduced by the new means of communication (and certain particular methods of sales promotion) used in contracts negotiated at a distance, the Commission highlights the need to supplement the mandatory basic rules by voluntary self-regulatory arrangements in the form of codes of practice.

Among other things, this recommendation provides important requirements regarding the information of consumers. Firms which subscribe to a code of conduct are notably required to inform their customers of this fact; consumers must therefore be able to acquaint themselves with the content of this code and should know what to do if they think it has not been complied with.

In general, the Recommendation provides the following requirements:

1. Adoption of codes of practice, with the particular aim of stating precisely, for the sectors concerned and means of communication used, the minimum rules contained in the Directive on 'contracts negotiated at a distance';
2. Inclusion of the points listed in the Annex in such codes;
3. Ensuring that their members comply with the codes;
4. Informing the Commission, one year after the publication of the Directive in the Official Journal of the European Communities, of the content of the codes and the response by their members.

Besides, it includes an annex which lists the points which could be covered by codes of practice for contracts negotiated at a distance such as:

- Dissemination of solicitations for custom: means to enable consumers not to receive solicitations if they have made it clear that they do not wish to do so;
- Presentation: ethical principles to be respected in all solicitations for custom, especially as regards respect for human dignity and religious or political beliefs.
- Sales promotion: provisions covering sales promotion techniques (reductions, rebates, gifts, lotteries and competition) to ensure that the principles of fair competition are respected and in particular that the consumer receives clear information;
- Financial security: arrangements to ensure the reimbursement of payments made by consumers at the time of placing an order;

7-10-1998, p.48. A number of indicative guidelines are annexed to this recommendation. These guidelines are aimed to ensure a full participation of all interested parties (public authorities, consumers, users and industries) in the drafting, implementation, evaluation and control of the respect of the codes of conduct. This participation is judged as necessary in order to legitimate the recourse to self regulatory solutions.

²⁹ In this regard, we significantly observe that mainly, on the one hand, the provisions regarding codes of conduct form a minor part of the concerned instruments, and on the other hand, the provisions do not impose a mandatory framework.

³⁰ The Commission Recommendation 92/295/EEC of 7 April 1992 on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling), *O.J.*, L 156, 10-06-1992, p.21.

- Right of withdrawal: if the consumer chooses to make use of the right of withdrawal, a period within which payments already made will be reimbursed;
- Knowledge of the code: information for consumers on the existence of the code, its content and the results of its application.

b) The Directive on distance contracts

In the field of distance selling practices, Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts³¹ also includes a short provision regarding codes of conduct.

Article 16 of the Directive states that:

“Member States shall take appropriate measures to inform the consumer of the national law transposing this Directive and shall encourage, where appropriate, professional organisations to inform consumers of their codes of practice”.

The EU encourages, once again, businesses to comply with a principle of transparency by requiring that consumers must be provided with information on the code of conduct.

c) The Directive on electronic commerce

The Directive 2000/31/EC on certain aspects of information society services, in particular e-commerce in the internal market contains two important provisions regarding codes of conduct³².

The first reference is part of the minimum information that must be given to consumers before placing an order. Indeed, some minimum information requirements are imposed on providers of information society services to ensure legal security and consumer confidence in electronic transactions.

In connection with codes of conduct, article 10, § 2 states that:

“Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically”.

Furthermore, the e-commerce Directive goes further than the Directive on distance contracts because article 10 imposes a strict obligation to information society services providers to provide information on codes of conduct. This article also states that the consumer should be able to consult those codes of conduct by electronic means.

Nevertheless, we may wonder whether it would have been more appropriate to include those requirements in the provision dedicated to “general information”³³, since every information society services providers can subscribe to a code of conduct, even those which provide non-transactional services.

³¹ O.J., n° L 144, 04-06-1997, p. 19.

³² P. DE LOCHT et CH. LAZARO, “Voyage dans les interstices du droit : autorégulation et codes de conduite dans le cadre du commerce électronique”, in *Le commerce électronique européen sur les rails ?* (E. MONTERO sous dir. de), Cahiers du CRID, n° 19, Bruxelles, Bruylant, 2001, pp. 297-326.

³³ Cf., Article 5 of Directive 2000/31/EC.

Another article of the e-commerce directive is entirely dedicated to codes of conduct.

Article 16 of the directive states:

“1. Member States and the Commission shall encourage:

(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;

(b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;

(c) the accessibility of these codes of conduct in the Community languages by electronic means;

(d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;

(e) the drawing up of codes of conduct regarding the protection of minors and human dignity.

2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted”.

In general, two requirements of article 16 are particularly important.

First, the Directive requires Member States to encourage the drawing-up and publication of codes of conduct. Recital 49 prudently adds that: *“this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes”.*

Secondly, the Directive suggests the application of what one could call a “principle of legitimacy” (guillemets). It requires Member States and the Commission to encourage the involvement of consumer organisations in the development and implementation of codes..

d) The proposal for Directive on unfair commercial practices

A recent proposal for a Directive of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the Internal Market³⁴ addresses some interesting issues regarding codes of conduct.

This proposal for a directive covers unfair commercial practices that affect the consumer’s economic interests. It aims to fully harmonize EU requirements relating to unfair business-to-consumer (B2C) commercial practices and provides an appropriately high level of consumer protection. Although not specific to online trading, this proposal is of major importance as it provides clear indications of the type of online commercial practices that would become outlawed.

³⁴ Proposal for a Directive of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the Internal Market and amending directives 84/450/EEC, 97/7/EC and 98/27/EC (the Unfair Commercial Practices Directive) COM(2003) 0356 final, http://europa.eu.int/eur-lex/en/com/reg/en_register_152040.html.

Within the framework of our survey, some provisions merit our particular attention.

- Article 2: definitions

This article defines a number of terms used in the directive. Among others, this article enlightens us about three typical concepts of self-regulation terminology: ‘code of conduct’, ‘Community level code’ and ‘code owner’:

“(g) ‘code of conduct’ means an agreement which defines the behaviour of the traders who undertake to be bound by the code in relation to one or more particular commercial practice or business sector;

(h) ‘Community level code’ means a code of conduct which allows any trader from any Member State, who meets the requirements laid down in the code, to participate on a non-discriminatory basis, and contains appropriate and effective mechanisms for monitoring and enforcing compliance with the code;

(i) ‘code owner’ means any entity, including a trader or group of traders, which is responsible for the formulation and revision of a code of conduct and/or for monitoring compliance with the code by those who have undertaken to be bound by it.

- Article 10: codes of conduct

This article is the single one composing Chapter 3 of the draft Directive, dedicated to codes of conduct:

“This Directive does not exclude the control which Member States may encourage, of unfair commercial practices by code owners of national or Community level codes and recourse to such bodies by the persons or organisations referred to in Article 11 if proceedings before such bodies are in addition to the court or administrative proceedings referred to in that Article”.

It aims to consider and define the role of the codes of conduct in the field of unfair commercial practices and, in particular, contains provisions for control of the Directive’s requirements by code owners.

As underlined in the explanatory memorandum³⁵, there is potential for codes with EU-wide application to promote convergence in expectations regarding professional diligence and thereby further reduce internal market barriers, while ensuring that such codes do not prevent, restrict or distort competition. Such codes could bring added value by helping traders to apply the principles in the Directive effectively in their particular day-to-day business.

Therefore, codes within the harmonised field of the Directive could be taken into account by the Member States in assessing whether a trader has breached the provisions of the Directive as implemented in the Member State where the trader is established. The precise way in which an EU code of conduct could operate would depend on the needs and circumstances of different sectors.

In this regard, Recital 14 of the draft directive adds that *“it is appropriate to provide a role for codes of conduct, which enable traders to apply the principles of the directive effectively in specific economic fields. Such codes may be helpful to national authorities in determining the*

³⁵ See n° 72 to 75 of the explanatory memorandum.

requirements of professional diligence in a particular sector. The control exercised by code owners at national or Community level to eliminate unfair commercial practices may avoid the need for recourse to administrative or judicial action and should therefore be encouraged”.

- Annex 1: blacklist of commercial practices

An Annex to the Directive contains a short blacklist of commercial practices. These are practices which will in all circumstances be considered unfair, and therefore banned in all Member States. This single list will apply to all Member States and can be changed or added to only in the same way as the rest of the Directive. This contributes to legal certainty and consumer confidence by imposing an *ex-ante* prohibition on those specific practices, such as pyramid schemes, which will always materially distort the decision-making of average consumers and are contrary to the requirements of professional diligence.

Two examples of **misleading commercial practices** concern codes of conduct³⁶:

- (1) Claiming to be a signatory to a code of conduct when the trader is not.
- (2) Claiming that a code of conduct has an endorsement from a public or other body which it does not have.

2.2.2 Trustmark schemes and EU regulations

Even though EU regulations do not directly address trustmark scheme issues, the latter nevertheless have to comply with general EU provisions applicable to their activities.

In our survey, we therefore identify the legal framework which applies to trustmark schemes. This identification work takes the form of an inventory that is fully integrated in the benchmark process. In such a way, we are able to verify to which extent the selected trustmark schemes meet the EU requirements.

As regards their organisation and functioning, this inventory is useful to assess the compliance of the trustmark schemes with, for instance, provisions of the e-commerce directive (e.g., regarding information), directive provisions concerning personal-data protection when they act as “information society service providers”, or as “data processors”, etc.

As regards the content of the code, this inventory serves to test the compliance with the principle of legality³⁷. The code of conduct imposed by the trustmark schemes on their subscribers should indeed, in any case, be in full compliance with EU regulations. In this view, trustmark schemes should comply fully with relevant EU legislation in relation to any obligation they place on subscribers or any practices they recommend to them. Furthermore, they should require that subscribers take the necessary steps to ensure their compliance with their legal obligations.

Codes of conduct may not seek to override or replace any mandatory provisions at European level, and therefore they may not affect consumers’ statutory rights.

Eventually, it allows us to determine the quality level of standards developed in each code of conduct associated with trustmark schemes. More particularly, it helps us to determine whether

³⁶ The proposal elaborates two key types of unfair commercial practice; those which are ‘misleading’ and those which are ‘aggressive’.

³⁷ An analogy can be made with the principle of legality contained in the Commission Recommendation 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes *O.J.*, n° L 115, 19-04-2001, p. 31.

codes are used only to show in greater detail how to apply legislative requirements (e.g., how to explain complex concepts in ways that consumers can understand) or to define norms or standards of behaviour for traders in areas where there are no specific legal requirements (e.g., aspects of after-sales care).

3. Quality Assessment of Trustmark schemes: selection of criteria

3.1. List of general criteria

In order to develop a model of trust that describes which legal factors affect the quality of a trustmark scheme, we do not limit our analysis to the single benchmarking of the content of the selected trustmark schemes' codes of conduct. We go further in adopting a more global perspective and covering the main aspects of this type of services.

For this reason, we elaborated a general list of criteria encompassing a number of criteria derived from various sources of regulatory instruments.

These regulatory instruments are:

- ∅ Sources of self-regulation (soft law)
 - European Trustmark Requirements (ETR);
 - Second draft principles for e-commerce codes of conduct (The E-Confidence Initiative Working Documents);
 - Global Business Dialogue on e-commerce Recommendations.

- ∅ Sources of EU law (hard law)
 - The Directive on distance contracts;
 - The Directive on electronic commerce;
 - The Directive on the protection of personal data;
 - The proposal for the Directive on unfair commercial practices;

From these different normative sources, including dispositions of hard and soft law, the highest common factors or criteria were identified. This comparative process resulted in the elaboration of a list of more than 40 general selection criteria³⁸. More information on this selection process and comments of criteria can be found in section four (4).

³⁸See, infra section 2. Also see Benchmark criteria; WP 2: List of relevant criteria and regulations.

3.2. A pragmatic approach: the life cycle of the scheme

Afterwards, the above mentioned general list was converted into a more functional synopsis. For the purpose of the phases of the “life cycle” of a trustmark scheme, *i.e.*, from conception, elaboration, dissemination to enforcement, different criteria were grouped and ordered in a more pragmatic and systematic manner.

The page numbers –on the right side of the list - refer to Section 3.4 of this deliverable concerning the normative source of the criteria and to some comments made to enhance common understanding.

1. ELABORATION OF THE TRUSTMARK SCHEME	27
1.1 <i>Legitimacy of the scheme</i>	27
1.2. <i>Code of conduct</i>	27
1.2.1. <i>Clearness</i>	28
1.2.2. <i>Multilingualism</i>	28
1.2.3. <i>Accessibility</i>	28
1.3 <i>Security</i>	29
2. INFORMATION ON THE TRUSTMARK SCHEME	32
2.1 <i>Identification of the trustmark scheme provider</i>	32
2.2. <i>General information on the trustmark scheme’s functioning</i>	33
2.2.1. <i>Trustmark scheme properties</i>	33
2.2.2. <i>Assessment procedure</i>	34
2.2.3. <i>Code of conduct</i>	34
2.2.4. <i>Subscribers participating in the trustmark scheme</i>	35
2.2.5. <i>Monitoring</i>	35
2.2.6. <i>Complaint procedure</i>	35
2.2.7. <i>Alternative dispute resolution</i>	35
2.2.8. <i>Sanctions/Remedies</i>	35
2.2.9. <i>Liability</i>	36
3. PARTICIPATION IN THE TRUSTMARK SCHEME.....	37
3.1. <i>Accessibility of the trustmark scheme</i>	37
3.1.1. <i>Open character</i>	37
3.1.2 <i>Affordability</i>	38
3.1.3 <i>Convenience</i>	38
3.2. <i>Procedure of assessment</i>	38
3.2.1 <i>Body in charge of the assessment</i>	39
3.2.2. <i>Quality of the assessment</i>	40
3.2.3. <i>Fairness of the assessment</i>	40
3.2.4. <i>Effectiveness of the assessment</i>	40
3.3. <i>Mutual recognition with other trustmark schemes</i>	40
4. CODE OF CONDUCT	41
4.1. <i>General principles</i>	41
4.1.1. <i>Trustmark localization</i>	41
4.1.2. <i>Transparency</i>	41
4.1.3. <i>Fairness and social responsibility</i>	43
4.1.4. <i>Applicable law and competent jurisdiction</i>	45
4.2. <i>Information on merchant</i>	46
4.2.1. <i>Identity of the service provider</i>	46
4.2.2. <i>Merchant’s commitments</i>	47

4.3. Information on products and services.....	48
4.3.1. Characteristics of the products or services.....	48
4.3.2. Prices.....	49
4.3.3. Supply restrictions	51
4.3.4. Delivery conditions.....	51
4.3.5. Guarantees.....	52
4.3.6. Duration of the contract	53
4.4. Conclusion of the contract.....	53
4.4.1. Contract terms and general conditions.....	53
4.4.2. Order procedure	54
4.4.3. Order error protections:	58
4.4.4. Cancellation/refund/return terms	58
4.4.5. Payment.....	61
4.4.6. Inertia selling/unsolicited services	62
4.4.7. Filing of the contract	62
4.5. Customer service.....	63
4.5.1. Information about customer service & contact point.....	64
4.5.2. Complaint procedure	64
4.5.3. Information on alternative dispute resolution.....	66
4.6. Commercial communications and fair marketing practices	68
4.6.1. Commercial communications.....	68
4.6.2. Fair marketing practices	69
4.6.3. Unsolicited commercial communications.....	70
4.7. Security of system and payment	72
4.7.1. Information on security policy and contact point.....	72
4.7.2. Implementation of technical requirements	73
4.8. Personal-data protection	75
4.8.1. Reference to privacy policy.....	75
4.8.2. Information.....	76
4.8.3. Notification to national DPA	77
4.9. Protection of children.....	77
4.9.1. Commercial communications and fair marketing practices	78
4.9.2. Harmful content	80
4.9.3. Personal-data protection.....	80
5. PROACTIVE MONITORING	81
5.1. Monitoring mechanisms.....	81
5.1.1. Fairness	81
5.1.2. Effectiveness	81
5.2. Monitoring reports.....	82
6. COMPLAINT PROCEDURE	83
6.1. Accessibility and convenience.....	83
6.2. Quality of the complaint procedure.....	83
6.2.1 Fairness	84
6.2.2 Effectiveness	84
6.3. Alternative dispute resolution	84
7. ENFORCEMENT SYSTEM	86
7.1 Quality of the enforcement process.....	86
7.1.1. Fairness	87
7.1.2. Effectiveness	87

8. RELATIONSHIPS WITH PROTAGONISTS	89
8.1. General relationships	89
8.1.1. Feedback	89
8.1.2. Report on activities	89
8.1.3. Additional services	89
8.2. Relationship with consumers	90
8.2.1. Validity of certification	90
8.2.2. Privacy Policy	90
8.3. Relationship with businesses	91
8.3.1. Promotion	91
8.3.2. Security and confidentiality	91

In conclusion, this list of criteria was used to identify a number of criteria a scheme should have to distinguish itself as a true legal quality seal.

3.3. “Must-have” vs. “Nice-to-have” criteria

For the purpose of the added value of soft law, we identified a number of legal criteria a trustmark scheme should meet to be recognized as a true legal quality label or self-regulatory instrument *i.e.*, the “**must-have**” criteria. All other criteria, derived from the various sources of hard and soft law, will be labelled “**nice-to-have**”. In contrast to the remaining list of “nice-to-have” criteria, the list of fourteen “must-have” criteria facilitates a better general understanding of the quality of a trustmark scheme and their respective position in relation to the other schemes. We, however, underline that this distinction is not always easy to make and is to a certain degree the result of a subjective selection process.

Although opinions may differ, this added-value criterion seems to be defensible. Of course all legal obligations, *e.g.*, of the Directive on electronic commerce, have to be respected. However, we advocate that for the evaluation of a trustmark scheme it is important to know to what extent the latter adds something new to an e-platform or the existing obligations of positive (hard) law. Indeed, we underline that criteria merely reflecting hard-law provisions should not be kept as “must-have” because scheme subscribers or members – by law – must comply with them. In other words, they are *in se* “must-have” criteria.

If for instance a Code of Conduct states that a member shall display its identity, we estimate that the added value of this “soft rule” is less³⁹ than when Members are required by the Code to have a proper customer service and adopt effective dispute-resolution procedures, subject to independent monitoring. Similarly, one could claim that a TMS elaborated by the different relevant stakeholders is more representative for an industry, and thus has more added value, than one that is conceived by an independent body without any consultation with the stakeholders, both businesses and consumers.










The list of “meta” or “must-have” criteria is the following;

1. Legitimacy of the scheme;
2. Clearness of the code of conduct;
3. Information on trustmark scheme’s functioning;
4. Feedback;
5. Assessment;
6. Applicable law and competent jurisdiction;
7. Confirmation process;
8. E-platform security;
9. Customer service;
10. Protection of children;

³⁹ Cf., *infra* on article 5 of the Directive on electronic commerce.

11. Proactive monitoring;
12. Compliant process for dispute resolution;
13. Enforcement system;
14. Relations with Consumers.

The table below shows i) the value given for each of the fourteen must-have criteria for each individual trustmark, ii) the aggregated value for each criteria and the iii) total score of each trustmark scheme.

	Labelsit	Safe Buy	Qweb	Webtrader	Webtrust	Trusted Shops	e-Lux Certified	Confianza	Thuis winkel waarborg	Criterion Score
1. Legitimacy of the scheme										
	2	5	1	3	1	5	5	3	4	64.44%
2. Access and clearness of the code of conduct										
	4	3	3	4.5	1	3.5	4	5	3	68.89%
3. Information on trustmark scheme's functioning										
	3.69	3.08	2.69	2.23	1.77	3.31	3.08	3.46	4	60.69%
4. Assessment										
	4.25	1.5	2.25	1.25	1.5	1.5	4	1.5	3	46.11%
5. Feedback										
	3	5	3	3	3	4	4	3	5	73.33%
6. Applicable law & competent jurisdiction										
	3	1	5	4	1	4	1	1	4	53.33%
7. Confirmation process										
	5	2	4	5	1	3	5	5	1	68.89%
8. E-platform security										
	3.5	5	5	2.25	1	3.5	4	4	4	71.11%
9. Customer service										
	3.25	3.5	4	4.5	1	2.5	3.25	3.5	3.25	63.89%
10. Protection of children										
	5	3.33	4.33	4.67	1	2.67	3.33	4	1	65.18%
11. Proactive Monitoring										
	3	1.67	2.33	2	1.33	2.33	3.33	1.33	1	40.71%
12. Complaints procedure for solving disputes										
	1	2.5	1.25	1.25	1	4	2.75	4.75	3.75	49.44%
13. Enforcement system										
	2	1.67	2.67	1.67	1	3	1	3	1.67	39.29%
14. Relationships with consumers										
	2	1.5	3	1.5	2	4.5	3.5	3.5	3	54.44%
TMS Score	63.84%	56.79%	62.17%	58.31%	26.57%	66.87%	67.49%	64.34%	59.53%	

3.4. Selection of and comments on benchmarking criteria

In order to develop a model of trust that describes which legal factors affect the quality of a trustmark scheme, we do not limit our analysis to a single benchmarking of the content of the selected trustmark schemes' codes of conduct. We go further in adopting a more global perspective and covering the main aspects of this type of services.

For this reason, we elaborated a general list of criteria encompassing a number of criteria contained in various sources of regulatory instruments.

These regulatory instruments are:

∅ Sources of self-regulation (soft law)

- European Trustmark Requirements (ETR);
- Second draft principles for e-commerce codes of conduct (The E-Confidence Initiative Working Documents);
- Global Business Dialogue on e-commerce Recommendations.

∅ Sources of EU law (hard law)

- The Directive on distance contracts;
- The Directive on electronic commerce;
- The Directive on the protection of personal data;
- The proposal for Directive on unfair commercial practices;

For a better understanding of each type of criterion, both "*nice-to-have*" and "*must-have*", we will go back to the normative sources concerned and briefly comment on their relation with the different life cycles of the trustmark scheme.

As indicated above, the following phases in the trustmark scheme's life cycle can be identified:

1. Elaboration of the trustmark scheme;
2. Information on the trustmark scheme;
3. Participation in the trustmark scheme;
4. Code of conduct;
5. Proactive monitoring;
6. Complaint procedure;
7. Enforcement;
8. Relationships with protagonists.

1. Elaboration of the trustmark scheme

1.1 Legitimacy of the scheme

This criterion applies to the elaboration phase of the trustmark program. It requires from the trustmark representatives to facilitate (?) or encourage the involvement of all interested parties (stakeholders), particularly the consumers, in the elaboration, drafting and implementation of the rules affecting the trustmark program and, in particular, the code of conduct.

Indeed the Global Business Dialogue on e-Commerce (GBDe) stresses that *“the most important elements in which dialogue among the different stakeholders is essential are the content of the code of conduct, enforcement mechanisms and redress measures”*.

In this regard, the presence of other organisations or public bodies, interactivity of merchant members, advisory body, businesses or consumer associations, EU Commission approved, public endorsement and support are important factors.

→ art. 16, § 2 Directive 2000/31/EC on electronic commerce (EC-D)

“Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted.”

→ art. 4 GBDe (C)

“Consumer, industry or professional organisations should ensure that they consult each other when developing trustmark programs.”

“The most important elements in which dialogue among the different stakeholders is essential are the content of codes of conduct, enforcement mechanisms and redress measures.”

1.2. Code of conduct

This criterion concerns the rules for drafting a code of conduct. Codes of conduct should be:

- Written in plain and intelligible language to facilitate comprehension by consumers and code subscribers;
- Well structured, e.g., using different subsections such as “definitions”, “obligations”, “dispute resolution”, etc.;
- Available in different languages with regard to the geographical scope of the trustmark scheme and the public concerned.

It is essential that the public concerned easily understands the content of the code of conduct and that they do not have to read it a number of times before they can understand what the scheme is about. In this regard, we stress that modern technologies, such as

printer-friendly web forms, pdf files, time stamping, links to relevant webpages, etc., can greatly contribute to the overall uniform understanding of a Trustmark scheme or a code of conduct.

→ art. 16, § 1 Directive 2000/31/EC on electronic commerce (EC-D)

16, § 1. “Member States and the Commission shall encourage:

(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15; (...)

(e) the drawing up of codes of conduct regarding the protection of minors and human dignity.”

→ Recommendation 92/295/EEC on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling) (CP-Rec)

“Hereby recommends:

That the trade associations of suppliers:

1. should adopt codes of practice, with the particular aim of stating precisely, for the sectors concerned and means of communication used, the minimum rules contained in the Directive on 'contracts negotiated at a distance'; (...).”

1.2.1. Clearness

→ art. 3, al. 1, e-Conf. General Principles

“Codes should be written in plain intelligible language to facilitate comprehension by consumers and code subscribers. Obligations on code subscribers should be formulated in terms as clear and precise as possible to avoid disputes arising over interpretation in the event of a breach of the code. (...).”

1.2.2. Multilingualism

→ art. 16, § 1 Directive 2000/31/EC on electronic commerce (EC-D)

16, § 1. Member States and the Commission shall encourage: (...)

(b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;

(c) the accessibility of these codes of conduct in the Community languages by electronic means; (...).”

1.2.3. Accessibility

It should be recommended that information is directly given on the website or in subsections of the website, e.g., code of conduct. The fact that information is given on the home page of the website will make it more direct than when this is done in a 'functional code of conduct as, e.g., in the case of Qweb. Furthermore, it should be possible to save the code on a durable support or to have a printer-friendly version available.

→ art. 10, § 2 Directive 2000/31/EC on electronic commerce (EC-D)

10, § 2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically

→ art. 3, al. 1, e-Conf. General Principles

“(…). Codes and decisions relating to the code made by code-owners should be made readily accessible in a timely fashion to the public.”

→ art. 6, § 1, e-Conf. Specific Guidelines

“(…). Code owners publicise the code to subscribers, consumer representatives and consumers and report on compliance with the code publicly. (…).”

1.3 Security

This criterion concerns the security issues related to the technological architecture of the trustmark scheme's website, in particular the integrity and confidentiality of communications. It aims to determine whether the trustmark scheme has put in place efficient technical solutions to ensure amongst others:

- The security of the website;
- The protection of the trustmark (to avoid fraudulent use of the trustmark);
- The protection of personal data (privacy) and of the communications exchanged between parties (confidentiality of communications);
- The security of communications, e.g., complaint entry, online trustmark membership registration, website login, protection of trade secrets and other sensitive business information.

In comparison with the related criteria 8.3.2 7 8.2.2, the present criterion 1.3 relates to the provision of information as such.

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 (DP-D), in particular:

→ art. 16 (Confidentiality of processing) and 17 (Security of processing) 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 (DP-D)

art. 16. “Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.”

art. 17. “1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

**- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.**

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.”

→ art. 4 (Security) and 5 (Confidentiality of the communications) Directive 2002/58/EC on privacy and telecommunications (PT-D)

art. 4. 1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

art. 5. “1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.”

→ section 9, al.2, ETR

“Information critical to establishing confidence, and in particular trustmarks, are authenticated using effective technical mechanisms.”

→ art. 5, § 2, GBDe (C)

“The certifier should take appropriate measures to maintain confidentiality of commercially sensitive information exchanged with the merchants it certifies.”

→ section 9, al.1, ETR

“Trustmark schemes should regularly report on fraudulent use of the trustmark.

→ art. 5, § 1, GBDe (C)

“The certifier should take appropriate measures to ensure that consumers can easily distinguish between real and counterfeit trustmarks. This may include technology to guarantee that unauthorized parties cannot copy the trustmark, secure links to a database accessible on the merchant’s website, or technology to monitor web pages that are displaying the trustmark.”

→ art. 9, al. 2, e-Conf. General Principles

“Code owners should pay particular attention to making it difficult, using available technology, to imitate the appearance and behaviour of trustmarks showing a code-subscriber’s membership of a code, both by non-members and by members whose status has lapsed.”

2. Information on the trustmark scheme

The criterion “information on trustmark scheme’s functioning” has to be taken in a very broad and general manner. It covers information on trustmark scheme properties, on the characteristics of assessment procedures, on subscribers participating in the trustmark scheme, information on enforcement mechanisms (monitoring, complaint handling, sanctions), etc.

It is important to stress that for methodological reasons, this criterion covers both the accuracy and the quality of information.

2.1 Identification of the trustmark scheme provider

In relation to information society services, the European Commission holds that additional regulatory provisions on the identification of the supplier should apply. In this view, *Directive 2000/31/EC on certain legal aspects of electronic commerce in the Internal Market* establishes general information to be provided by the service provider regardless of whether a contract is going to be concluded or not. In this respect, it complements and further specifies Community provisions relating to the identity of the service provider.

The electronic commerce Directive stipulates that providers of information society services will have to render easily accessible, in a direct and permanent manner, information such as the name of the service provider, the address at which the service provider is established, the particulars of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner, etc.

This information obligation would be more stringent than that applying to traditional (off-line) (distance) commerce. In order to ensure and stimulate consumer confidence in electronic commerce, and bearing in mind the special characteristics of the technology and of information society services, this obligation can be justified.

→ art. 5, § 1 (General information to be provided) Directive 2000/31/EC on electronic commerce (EC-D)

“1. In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:

(a) the name of the service provider;

(b) the geographic address at which the service provider is established;

(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(f) as concerns the regulated professions:

- any professional body or similar institution with which the service provider is registered,

- the professional title and the Member State where it has been granted,

- a reference to the applicable professional rules in the Member State of establishment and the means to access them;

(g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment(29)."

2.2. General information on the trustmark scheme's functioning

This section concerns the general information that should be provided by the trustmark scheme regarding the different modalities and characteristics of its functioning.

The methodology used for this section is based on an evaluation of both the accuracy and the quality of information. For each criterion, these two aspects are analysed and evaluated simultaneously. Regarding the quality of information, we take into account characteristics such as the clearness, the accessibility of information, *i.e.*, the information should be easily and clearly accessible to the visitors of the trustmark scheme's website.

One may encounter problems when information is only found in a code of conduct and not directly on the website. In this case, the information will be present, the quality may be good, but it could be difficult to find. We hold that quality information that cannot be found, *e.g.*, via a direct link on the home page, should not be evaluated as too positive.

→ section 2 “Transparency of trustmark schemes for consumers and business”, ETR

“Trustmark schemes should provide information about themselves. They should publish and make clear to both consumers and business:

- the criteria for participation in the trustmark scheme,***
- the trustmark scheme requirements,***
- the subscribers participating in the trustmark scheme and***
- the identity of the independent third party.***

Trustmark schemes should publish an annual report on their activities.

Trustmark schemes should use plain and intelligible language that is easy to understand.

Information provided at any stage should be presented in a clear, concise, intelligible, timely, accurate and easy accessible manner.”

2.2.1. Trustmark scheme properties

2.2.1.1. scope and objectives

What is the objective of the trustmark scheme? It is to ensure compliance with hard-law provisions, dispute mediation or facilitating alternative third-party dispute resolution. The scope of the trustmark scheme relates more to the criteria for participation and who can become a member.

2.2.1.2. management

Is there information regarding the persons behind the scheme? Provide name, profile, functions, contact details, management structure, etc.

→ art. 1, § 2, GBDe (C)

“(…). The criteria for participation in a trustmark program should be transparent to applicants and to consumers.”

2.2.2. Assessment procedure

2.2.2.1. type and subject of the procedure

An audit and additional information on the assessment procedure such as the intervention of an independent body, time, costs, assessment criteria are very important.

2.2.2.2. identity, composition and role of the assessment body

2.2.2.3. costs

→ section 6, ETR

“Trustmark schemes should have a clear procedure in place for the assessment of applicants for trustmark schemes.

→ art. 7, § 2, GBDe (C)

“The certifier should have all the necessary information about the requirements to join the program available on-line or in an electronic version. This information should be provided in a simple manner to ensure easy comprehension of the terms of participation.”

2.2.3. Code of conduct

2.2.3.1. normative references

The object of this criterion is the normative references which regulate the various aspects of a code of conduct. The trustmark scheme should inform the parties about the main legislative references the code is based on. In this regard, it is important that detailed information is given on the regulatory framework, not just the mere fact that Belgium law applies.

→ Recommendation 92/295/EEC on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling) (CP-Rec)

“Hereby recommends:

That the trade associations of suppliers:

1. should adopt codes of practice, with the particular aim of stating precisely, for the sectors concerned and means of communication used, the minimum rules contained in the Directive on 'contracts negotiated at a distance'; (...).”

2.2.3.2. update

This criterion concerns the review of the code in order to reflect the most recent legislative and market developments. In this respect the code should be regularly reviewed and updated and the parties notified of any change. It is subsequently important to check whether information regarding the potential review of the Code is indeed provided, as well as frequency, review dates or versions.

It is also important to see whether codes of conduct are time stamped, this in particular with regard to dispute mediation and resolution.

→ art. 2, al. 3, e-Conf. General Principles

“Codes should be up-to-date, reflecting most recent market practice. (...)”

→ art. 6, § 1, e-Conf. Specific Guidelines

“(...) Code owners carry out a periodic review and updating of the code.”

2.2.4. Subscribers participating in the trustmark scheme

→ art. 7, § 4, GBDe (C)

“(...) The certifier must include a list of all certified merchants that must be prominently shown in the trustmark program web page.”

2.2.5. Monitoring

It is important that a direct link or entry to the relevant information on monitoring is given.

2.2.6. Complaint procedure

2.2.7. Alternative dispute resolution

It is important that a direct link or entry to the relevant information on the intervention of third-party dispute resolution body is given.

2.2.8. Sanctions/Remedies

→ section 8, al. 3 and 5, ETR

al. 3. “A list of dissuasive and proportionate sanctions should be established, which could include information to the media and financial fines.”

al. 5. “The enforcement process should be transparent.”

→ art. 2, § 4, GBDe (C)

“The certifier should disclose publicly and prominently the type of actions that it will undertake in order to ensure compliance with the program.”⁴⁰

2.2.9. Liability

Although the liability of all service providers, including trustmark scheme operators, is important, we underline that this criterion is very difficult to assess. In contrast to other criteria, one should be aware that a liability disclaimer of information regarding the limited scope of liability of the scheme operator could have a reverse, even perverse, effect. Indeed, the final objective of each trustmark scheme is to create and enhance consumer confidence, which seems to be in contradiction with a too explicit information notice or disclaimer on liability.

In this view, we formulate the following thoughts.

- The scope of scheme liability, is implicitly determined by the scope of the objective. Unless otherwise stated, it seems illogical that a trustmark scheme will also guarantee the quality of the products of the merchant member.
- Instead of a liability disclaimer, we estimate that a liability confirmation does not have such a strong reverse effect. However and changing a viewpoint, an explicit guaranty of liability confirmation implicitly excludes the non-covered liability items of its scope.

Eventually, we stress that if no information is given, liability will be appraised according to the general liability principles of common law.

⁴⁰ See also art. 2, § 2, GBDe (C): “The certifier should clearly include in the contract with the merchant the type of actions that will be undertaken if the merchant does not comply with the program requirements.”

3. Participation in the trustmark scheme

3.1. Accessibility of the trustmark scheme

This criterion concerns the modalities offered to the applicants to join the trustmark scheme. In this respect, the trustmark scheme should be:

- Open to any interested professional organisation;
- Affordable: subscription fees should not constitute an insurmountable obstacle to join the program (especially for SME's);
- Convenient: the opportunity to apply for the trustmark program should be offered on-line. This does not preclude the possibility to undertake physical checks.

3.1.1. Open character

This criterion aims to evaluate whether participation in a trustmark scheme is open to any interested organisation or person, regardless of their place of establishment.

In other words, is participation in the scheme strictly limited to merchants established in the country of origin of the scheme or is it broader? Does the trustmark scheme take into account the trans-national character of e-commerce? Can a merchant established in a foreign country become a scheme subscriber if his activities are directed towards the country of origin of the trustmark scheme?

Moreover, is the participation in the scheme open to all types of merchants, to other types of services providers (non-transactional websites), etc.?

→ section 3, § 2, ETR

“Subscription to a trustmark scheme should, in principle, be open to any interested organisation or person, regardless of their place of establishment. (...).”

→ art. 1, § 2, GBDe (C)

“Participation in a trustmark program should be open to any organization that agrees to abide by the entry conditions, consistent with the legitimate business objectives of the certifier. (...).”

→ art. 4, al. 1, e-Conf. General Principles

“Subscription to a code should, in principle, be open to any interested organisation or person, regardless of their place of establishment. (...).”

3.1.2 Affordability

From a certain point of view, this criterion should also be considered together with the commercial viability of a trustmark scheme.

→ art. 1, §§ 3 and 4, GBDe (C)

§ 3. “Subscription fees should not constitute an insurmountable obstacle to join a trustmark program. This should not discourage the setting up of additional fees for specific value-added services.”

§ 4. “Certifiers are encouraged to offer specific conditions for SMEs in order to facilitate the participation of SMEs in a trustmark program.”

3.1.3 Convenience

Is it possible to apply for membership online? Is the registration process user-friendly? What is the content of the application form?

→ art. 7, § 3, GBDe (C)

“(…). It is desirable that all steps to join a trustmark program can be conducted on-line. This does not preclude the necessity to undertake physical checks (e.g. about the real existence of the organization).”

3.2. Procedure of assessment

This criterion especially concerns the quality of the assessment mechanisms. In this regard, special attention must be paid to the nature of the body in charge of the assessment, notably its composition and independence. We note that the assessment procedure is the first step in ensuring a well-enforced trustmark scheme. With regard to the independence of the assessment body, we note that this body may operate within the trustmark scheme as long as there are sufficient guarantees that there is an internal “separation of powers” between the different structures and bodies, e.g., management, dispute-resolution body, General Assembly, etc.

→ section 5, ETR

“Trustmark schemes must have the resources necessary to assess applicants, to operate a trustmark scheme and to deal with complaints regarding non-compliance with the trustmark requirements.”

→ art. 2, e-Conf. General Principles

“Codes should comply fully with all relevant EU legislation in relation to any obligations they place on code-subscribers or any practices they recommend to them and should require that code-subscribers take the necessary steps to ensure their compliance with their legal obligations.”

Codes should add value for consumers and code-subscribers through complementing and supplementing legal obligations. In achieving this and in particular when addressing industry-specific issues, codes may repeat, refer to or provide guidance on legal obligations to enable code-subscribers to comply with them, provided that codes do not misrepresent or purport to give authoritative interpretations and include appropriate disclaimers to that effect.

(...). Codes should promote high standards of customer service by code-subscribers in terms of their responsiveness, flexibility, openness and timeliness in all their dealings with consumers.”

3.2.1 Body in charge of the assessment

This section concerns the legitimacy of the body in charge of the assessment. In this respect, two items need to be analysed: its independence and the competence of its members and assessors.

3.2.1.1. Independence of the body

3.2.1.2. Competence of the assessors

→ section 3, § 2, ETR

“(...). Any decisions to accept or reject applicants as subscribers should not be discriminatory and should be based on transparent membership criteria. ”

→ art. 7, § 3, GBDe (C)

“The certifier should take all reasonable steps to ensure a speedy decision on participation in the program by the applicant organization. It is desirable that all steps to join a trustmark program can be conducted on-line. This does not preclude the necessity to undertake physical checks (e.g. about the real existence of the organization).”

→ art. 4 and art. 7, e-Conf. General Principles

art. 4. “(...). Code-owners’ decisions to accept or reject applicants as subscribers to the code should be neither discriminatory nor anti-competitive, and be based on transparent and pre-existing membership criteria.

The code owner must demonstrate independence, impartiality and objectivity in all its decisions, notably to grant or withdraw membership of a code; or appoint an independent body to take these decisions. These decisions must be independently verifiable. The code owner should separate its responsibilities as code-owner from any other activities it performs especially where conflicts of interest may arise.”

art. 7. “Before granting certification or approval to code-subscribers, code owners should take the necessary steps to ensure that code-subscribers comply fully with the provisions of the code. (...).”

3.2.2. Quality of the assessment

This criterion aims to evaluate the quality of the assessment procedure. Such procedure should be:

- Fair to and transparent for the subscribers;
- Based on effective methods: the effectiveness of the scheme can be evaluated regarding 1) the quality level of the standards used for the assessment and 2) the assessment mechanisms (check of the relevant website, of the corporate identity and its internal procedures to ensure compliance, etc.).

3.2.3. Fairness of the assessment

3.2.4. Effectiveness of the assessment

3.2.1.1. Time-span

3.2.1.2. Methods

→ section 6, ETR

“Trustmark schemes should have a clear procedure in place for the assessment of applicants for trustmark schemes.

This should be done through an assessment of the applicant’s compliance with the trustmark requirements which should include a check of the applicant’s relevant website, its corporate identity and its internal procedures to ensure compliance.”

3.3. Mutual recognition with other trustmark schemes

The objective of this criterion is to examine whether the analysed trustmark scheme has put in place specific mechanisms to develop mutual recognition or similar arrangements with other trustmark schemes from other countries or regions.

→ art. 7, § 5, GBDe (C)

“The certifier should consider developing mutual recognition or similar arrangements with trustmark programs in other countries or regions, such that merchants certified under one program that complies with these guidelines can be identified by consumers in other jurisdictions as offering equivalent protection.”

4. Code of conduct

4.1. General principles

4.1.1. Trustmark localization

This criterion serves to examine whether the trustmark schemes specify in their code of conduct the mode of display of the trustmark seal and its location on the merchant's website. These aspects should be regulated to allow consumers to easily verify membership, the validity of the seal and to determine its purpose, scope and standards.

→ section 3, al. 1, ETR

“The Trustmark should be easily visible to the consumer. (...).”

→ art. 3, § 2, GBDe (C)

“The trustmark should be prominently visible to the consumer in any of the following locations:

- *on the welcome page of the merchant's web site;*
- *in case of privacy trustmarks, at a stage in the transaction prior to the collection of personal data from consumers;*
- *on the page where vendors or consumers initiate a transaction by making a clear offer.”*

→ art. 3, § 1, GBDe (C)

“The certifier should advise the merchant about suitable locations for the trustmark.”

→ art. 6, § 3, e-Conf. Specific guidelines

“Codes should require that their trustmarks or any form of identification of membership of a code incorporate links to the related websites so that consumers can easily verify membership and determine its purpose, scope, and standards.”

Code subscribers conform with the code's rules on the display, activation and uses of the trustmark or any form of identification of membership of a code.”

4.1.2. Transparency

The objective of this criterion is to insist on the quality of information that the merchant provides to its customers. The code should require subscribers to provide this information:

- In a clear and comprehensible manner (easily, directly, unambiguously and permanently accessible);
- In the languages used to offer goods and services.

4.1.2.1 Clear information

→ art. 5, § 1 and 10, § 1 Directive 2000/31/EC on electronic commerce (EC-D)

art. 5, § 1. “In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: (...)”.

art. 10, § 1. “In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service: (...)”.

→ art. 4, § 2 Directive 97/7/EC on distance contracts (DC-D)

“The information referred to in paragraph 1, the commercial purpose of which must be made clear, shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions, and the principles governing the protection of those who are unable, pursuant to the legislation of the Member States, to give their consent, such as minors.”

→ art. 3, § 2 Directive 2002/65/EC on financial services (FS-D)

→ art. 1, § 1, GBDe (M)

“All information required to be disclosed by the merchant shall be clear, accurate, and easily accessible online. The information shall either be posted on or accessible through a hyperlink from the merchant’s homepage or entry point of the online site or at a place where the transaction is offered.”

→ art. 3, al. 2, e-Conf. General Principles

“Codes should require that code-subscribers act in an open and transparent way in all their relations with consumers and code-owners. Information provided at any stage should be presented in a clear, concise, intelligible, conspicuous, timely, accurate and easily accessible manner. Such information should be sufficient for informed purchasing decisions (and other matters related to the transaction) and be capable of retention by the consumer in a durable medium.”

4.1.2.2. Language and global dimension

Trustmark schemes must require that subscribers agree to communicate in the language used for offering goods and services, throughout the contractual relationship, including the general terms and conditions and complaints settlement procedures.

→ art. 10, § 1, d) Directive 2000/31/EC on electronic commerce (EC-D)

“1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service: (...) (d) the languages offered for the conclusion of the contract.”

→ art. 3, § 1, 3), g Directive 2002/65/EC on financial services (FS-D)

“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning: (...)

3) the distance contract

(g) in which language, or languages, the contractual terms and conditions, and the prior information referred to in this Article are supplied, and furthermore in which language, or languages, the supplier, with the agreement of the consumer, undertakes to communicate during the duration of this distance contract; (...)”

→ section 4, § 1, ETR

“Subscribers must use plain and intelligible language.

Trustmark schemes must require that subscribers agree to communicate in the language used for offering goods and services, throughout the contractual relationship, including the general terms and conditions and complaints settlement procedures.”

→ art. 5, § 1, GBDe (M)

“Material information about the transaction shall be provided in the same language in which the good or service is offered. The use of automatic language programs for translation purposes should be encouraged. (...).”

→ art. 5 and 6, al. 1, e-Conf. General Principles

art. 5. “Codes should take into account the requirements of cross-border shopping. In order to achieve this aim they should be relevant and meaningful to consumers and businesses irrespective of where the consumer or the business is located.

Codes should require that code-subscribers act in a consistent manner in their choice of language, throughout the relationship with the consumer. The consumer should be able to use the same language or languages to conclude contracts, complain or seek redress. Codes should require that code-subscribers draw this to consumers' attention.”

art. 6, al. 1. “Codes should require that code-subscribers give due respect to all potential consumers whatever their race, nationality, gender, age, sexual orientation or religious belief (...).”

4.1.3. Fairness and social responsibility

This criterion, which has a general character, focuses on the social role of the merchant in the information society. In this respect, the code should require subscribers not to encourage behaviour prejudicial to health or safety or human dignity. We shall consider whether the social role of the merchant meets particular requirements, e.g., regarding adult content, harmful sites, human dignity and protection of minors. In short, we will assess the social role and function of Merchants.

→ Proposal for a Directive concerning unfair business-to-consumer commercial practices in the Internal Market (UCP-Prop D)

→ Recommendation 92/295/EEC on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling) (CP-Rec)

See Annex “Points which could be covered by codes of practice for contracts negotiated at a distance”: (...)

“- Presentation: ethical principles to be respected in all solicitations for custom, especially as regards respect for human dignity and religious or political beliefs. (...)”

→ Recommendation 98/560/EC on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (M-Rec)

“II. RECOMMENDS that the industries and parties concerned: (...)

(2) cooperate in the drawing up of codes of conduct for the protection of minors and human dignity applying to the provision of on-line services, inter alia to create an environment favourable to the development of new services, taking into account the principles and the methodology described in the Annex; Member States and parties concerned in the various fields covered by this recommendation; (...).”

See also Annex “Indicative guidelines for the implementation, at national level, of a self-regulation framework for the protection of minors and human dignity in on-line audiovisual and information services”:

“2.2.2. Protection of human dignity

Objective: to support effective measures in the fight against illegal content offensive to human dignity.

(a) Information for users

Objective: where possible, users should be clearly informed of the risks inherent in the use of on-line services as content providers so as to encourage legal and responsible use of networks.

Codes of conduct should address, for example, the issue of basic rules on the nature of information to be made available, its timing and the form in which it is to be communicated.”

→ Decision N° 276/1999/EC of 25 January 1999 ‘adopting a multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (IHC-De)

→ art. 1, al. 2, art. 2, al. 1 and art. 6, e-Conf. General Principles

art. 1, al. 2. *“Codes should require code-subscribers to ensure that, even if the representations they make or practices they engage in may differ between on-line and off-line situations, these differences do not result in a lower level of consumer protection for on-line consumers.”*

art. 2, al. 1. *“Codes should (...) require that code-subscribers take the necessary steps to ensure their compliance with their legal obligations.”*

art. 6. *“Codes should require (...) that where information or images transmitted by them may be offensive, they provide suitable warnings.*

Code subscribers should not encourage behaviour prejudicial to health or safety, protection of the environment or human dignity.”

4.1.4. Applicable law and competent jurisdiction

This criterion aims to analyse whether codes contain specific requirements for merchants to provide information, concerning the law applicable to the contract and the competent jurisdiction, in case of a dispute. In line with Article 3 of the electronic commerce Directive, information society service providers are only subject to the law of the Country of Origin (place of establishment).

However, the electronic commerce Directive and Private International law include derogations of the Country of Origin principle and, in principle, consumers cannot be deprived from the protection offered by their national law.

Therefore, we shall also consider whether in a B2C relation information on (foreign) consumer-protection legislation or reference to the fact that a consumer cannot be deprived from the protection offered by his national law, is given.

→ art. 3, § 1, 3) e-f Directive 2002/65/EC on financial services (FS-D)

“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning: (...)

3) the distance contract

(e) the Member State or States whose laws are taken by the supplier as a basis for the establishment of relations with the consumer prior to the conclusion of the distance contract;

(f) any contractual clause on law applicable to the distance contract and/or on competent court; (...).”

→ art. 5, § 2, GBDe (M)

“Merchants shall make available to consumers the terms and conditions applicable to the transaction. Such information should include:

• (...)

• information about any self-regulatory programs to which the merchant adheres, and how to access those rules, and notice on the law applicable to the commercial relation (...).”

4.2. Information on merchant

4.2.1. Identity of the service provider

The objective of this criterion is to identify the provider of goods or services in order to meet the customer's need to know information such as name, physical business location, e-mail address, phone number, VAT number, etc.

→ art. 5, § 1 (General information to be provided) Directive 2000/31/EC on electronic commerce (EC-D)

“In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:

(a) the name of the service provider;

(b) the geographic address at which the service provider is established;

(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(f) as concerns the regulated professions:

- any professional body or similar institution with which the service provider is registered,

- the professional title and the Member State where it has been granted,

- a reference to the applicable professional rules in the Member State of establishment and the means to access them;

(g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment(29).”

→ art. 5, § 1, a) Directive 97/7/EC on distance contracts (DC-D)

“1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information:

(a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address; (...).”

→ art. 3, § 1, 1) Directive 2002/65/EC on financial services (FS-D)

1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning:

1) the supplier

(a) the identity and the main business of the supplier, the geographical address at which the supplier is established and any other geographical address relevant for the customer's relations with the supplier;

(b) the identity of the representative of the supplier established in the consumer's Member State of residence and the geographical address relevant for the customer's relations with the representative, if such a representative exists; (...).”

→ section 4, § 4, pt. 1, ETR

“Consumers should be given information concerning the subscriber including name, telephone number, postal and electronic-mail addresses. Information on the office hours or times when telephone contact can be made should also be given.”

→ art. 3, § 1, GBDe (M)

“Merchants should provide, at a minimum, the following contact information online:

- *legal name;*
- *the name(s) under which it conducts business;*
- *the principal physical address, addresses of representative offices in other countries or other information sufficient to ensure the customer can locate the business offline;*
- *an online method of contact such as email;*
- *a point of contact within the organization that is responsible for customer inquiries; and*
- *a telephone number, unless to do so would be disruptive to the operation of the business given its size and resources and then the merchant should maintain a working listed phone number, the time zone in which it operates, and the hours when contact may be made.”*

→ art. 2, § 1, e-Conf. Specific Guidelines

“Consumers are given a point of contact and information on hours of operation.”

4.2.2. Merchant’s commitments

This criterion concerns the disclosure to consumers of information regarding the different merchant’s commitments to third parties such as a code owner (reference to a code of conduct) and the trust certifications obtained by the merchant (quality of the products, environmental, energy).

→ art. 10, § 2 Directive 2000/31/EC on electronic commerce (EC-D)

“Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.”

→ art. 16 Directive 97/7/EC on distance contracts (DC-D)

“Member States shall take appropriate measures to inform the consumer of the national law transposing this Directive and shall encourage, where appropriate, professional organizations to inform consumers of their codes of practice.”

→ Recommendation 92/295/EEC on codes of practice for the protection of consumers in respect of contracts negotiated at distance (distance selling) (CP-Rec)

See Annex *“Points which could be covered by codes of practice for contracts negotiated at a distance”*: (...)

“- Knowledge of the code: information for consumers on the existence of the code, its content and the results of its application.”

→ art. 5, § 2, GBDe (M)

“Merchants shall make available to consumers the terms and conditions applicable to the transaction. Such information should include:

- (...)
- ***information about any self-regulatory programs to which the merchant adheres, and how to access those rules, and notice on the law applicable to the commercial relation (...).”***

4.3. Information on products and services

This section focuses on the description and the presentation of the products and services offered by the merchant. Prior to the conclusion of any distant contract, the consumer must be provided with information on the following issues. A code should therefore require the merchant to:

- Provide a clear description of the technical and qualitative characteristics of the products and services;
- Make it possible to verify (on-line) the availability of the goods or services;
- Ensure that prices are transparent, without hidden costs such as taxes, packaging or delivery costs;
- Give a clear specification of the terms of the validity of the supply, including geographical and temporal restrictions;
- Give a clear specification of the delivery conditions (means, place and delay of delivery, maximum time limits, ...);
- Give a clear definition of the guarantees offered on the products or services;
- Give a clear specification of the duration of the contract.

4.3.1. Characteristics of the products or services

4.3.1.1. clear description of the technical and qualitative characteristics of the products/services

→ art. 4, § 1, b) Directive 97/7/EC on distance contracts (DC-D)

“1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (...)

(b) the main characteristics of the goods or services; (...).”

→ art. 3, § 1, 1) Directive 2002/65/EC on financial services (FS-D)

“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning: (...)

2) the financial service

(a) a description of the main characteristics of the financial service; (...).”

→ section 4, § 4, pt. 2, al. 1, ETR

“Subscribers should provide all relevant information about the goods and services on offer in qualitative and quantitative terms. (...).”

→ art. 2, § 2, al. 1, e-Conf. Specific Guidelines

§ 2, al. 1. “Consumers are given all relevant information about the product or service on offer in qualitative and quantitative terms. This should include, for example, health and safety warnings, [label information] and any geographical restrictions on purchase.”

4.3.1.2. availability of the products/services

→ section 4, § 4, pt.4, ETR

Pt. 4. “Supplementary to all legally required information and other relevant information the subscriber must provide the following information:

- (...)
- Regularly updated information about the availability of the good or service and the time for delivery;
- (...).”

→ See art. 1, § 1, GBDe (M)

“Merchants shall provide enough information about the goods or services available online so that consumers can make an informed choice about whether to engage in a transaction online.”

→ art. 2, § 3, al. 3, e-Conf. Specific Guidelines

“Consumers are given information about the availability of the good or service, the due date for shipment and the likely arrival date.”

4.3.2. Prices

Prices must be stated in a clear manner, without pitfalls such as a hidden currency exchange rate or packaging or delivery costs.

→ art. 5, § 2 Directive 2000/31/EC on electronic commerce (EC-D)

“In addition to other information requirements established by Community law, Member States shall at least ensure that, where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.”

→ art. 4, § 1 Directive 97/7/EC on distance contracts (DC-D)

“1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (...)

(c) the price of the goods or services including all taxes; (...)

(d) delivery costs, where appropriate;

(g) the cost of using the means of distance communication, where it is calculated other than at the basic rate;

(h) the period for which the offer or the price remains valid; (...).”

→ art. 3, § 1, 2) Directive 2002/65/EC on financial services (FS-D)

“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning:

2) the financial service (...)

(b) the total price to be paid by the consumer to the supplier for the financial service, including all related fees, charges and expenses, and all taxes paid via the supplier or, when an exact price cannot be indicated, the basis for the calculation of the price enabling the consumer to verify it;

(d) notice of the possibility that other taxes and/or costs may exist that are not paid via the supplier or imposed by him;

(g) any specific additional cost for the consumer of using the means of distance communication, if such additional cost is charged.”

→ Directive 98/6/EC on the indication of the prices of products offered to consumers (IP-D), notably:

art. 3, § 1. “The selling price and the unit price shall be indicated for all products referred to in Article 1, the indication of the unit price being subject to the provisions of Article 5. The unit price need not be indicated if it is identical to the sales price.”

art. 4, § 1. “The selling price and the unit price must be unambiguous, easily identifiable and clearly legible. Member States may provide that the maximum number of prices to be indicated be limited.”

→ section 4, § 4, pt. 2, al. 3 and 4, ETR

“Subscribers should indicate the currency in which the good or service is priced and other currencies available for use.

Information should be given on the total costs collected and/or imposed by the subscriber. Where costs are not collected or imposed by subscribers, notice of their existence and, where possible, a scale of these charges should be indicated. ”

→ art. 5, § 3, GBDe (M)

“Merchants shall disclose the entire price of goods and services and any other charges to be collected by the merchant. Such information should be provided in a specified currency and should include:

- price or license fee to be charged, including all taxes, or in the case of a barter trade, the items that will be exchanged for goods or services purchased or licensed;***
- shipping and handling charges***

Merchants shall honour the amount authorized by the consumer in any subsequent bill to the customer.”

→ art. 2, § 2, al. 2 and 3, e-Conf. Specific Guidelines

al. 2. “The currency or currencies used are stated.”

al. 3. “As far as possible, additional charges which may be levied (e.g. customs duties) are indicated.”

4.3.3. Supply restrictions

→ art. 4, § 1, h) Directive 97/7/EC on distance contracts (DC-D)

“1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (...)

(h) the period for which the offer or the price remains valid; (...).”

→ section 4, § 4, pt. 2, al. 2, ETR

“Any geographical restrictions on sale must be prominently indicated.”

→ art. 5, § 2, GBDe (M)

“Merchants shall make available to consumers the terms and conditions applicable to the transaction. Such information should include:

- ***any restrictions or limitations (for example, time or geographic) they impose on the commercial offer and/ or the sale of the goods or services;***
- ***(...).”***

→ art. 2, § 2, al. 1, e-Conf. Specific Guidelines

“Consumers are given all relevant information about the product or service on offer in qualitative and quantitative terms. This should include, for example, health and safety warnings, [label information] and any geographical restrictions on purchase.”

4.3.4. Delivery conditions

What are the terms for product delivery, especially the means, place and delay of delivery, maximum time limits, etc.

→ art. 4, § 1, e) Directive 97/7/EC on distance contracts (DC-D)

“1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (...)

(e) the arrangements for payment, delivery or performance; (...).”

→ art. 5, § 4, GBDe (M)

“Merchants shall disclose to consumers when they will be able to ship the goods or provide services, and the expected time when a consumer’s credit card will be charged for a transaction. A consumer shall not be charged for a product or service unless shipment of such product or service is expected within a reasonable period of time.

In particular, merchants should:

- ***state which products or services are temporarily unavailable and if an expected availability date is provided, have a reasonable basis for such date;***
- ***have a reasonable basis for, and provide consumers with, estimated shipping times (or in the case of online delivery, delivery times);***
- ***have a reasonable basis for stated delivery claims when made; and***
- ***disclose any shipping, performance, or delivery limitations they impose (age, geographic).***

If a material delay in shipping or performance occurs, the merchant shall provide the consumer with information about the delay and the opportunity to cancel the transaction. ”

→ art. 2, § 3, al. 3, e-Conf. Specific Guidelines

“Consumers are given information about the availability of the good or service, the due date for shipment and the likely arrival date.”

4.3.5. Guarantees

Is a clear definition of the guarantees offered on the products or services given?

→art. 6 Directive 1999/44/EC on the sale of consumer goods and associated guarantees (GG-D)

“1. A guarantee shall be legally binding on the offerer under the conditions laid down in the guarantee statement and the associated advertising.

2. The guarantee shall:

- *state that the consumer has legal rights under applicable national legislation governing the sale of consumer goods and make clear that those rights are not affected by the guarantee,*
- *set out in plain intelligible language the contents of the guarantee and the essential particulars necessary for making claims under the guarantee, notably the duration and territorial scope of the guarantee as well as the name and address of the guarantor.*

3. On request by the consumer, the guarantee shall be made available in writing or feature in another durable medium available and accessible to him.

4. Within its own territory, the Member State in which the consumer goods are marketed may, in accordance with the rules of the Treaty, provide that the guarantee be drafted in one or more languages which it shall determine from among the official languages of the Community.

5. Should a guarantee infringe the requirements of paragraphs 2, 3 or 4, the validity of this guarantee shall in no way be affected, and the consumer can still rely on the guarantee and require that it be honoured.”

→ art. 5, § 2 and art. 9, § 1, GBDe (M)

art. 5, § 2. “Merchants shall make available to consumers the terms and conditions applicable to the transaction. Such information should include:

- (...)
- *for goods, any warranties, guarantees, escrow programs or other offered terms, including limitations, conditions;*
- *for services, any standards, schedules, fees, or other offered terms, including limitation and conditions; (...).”*

art. 9, § 1. “Merchants shall disclose to consumers applicable warranties or limited warranties that they offer regarding the goods or services sold or made available to consumers. Such information should include the scope, duration, and means of exercising rights made available in the warranty or limited warranty.”

4.3.6. Duration of the contract

→ art. 4, § 1, i) Directive 97/7/EC on distance contracts (DC-D)

“1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (...)

(i) where appropriate, the minimum duration of the contract in the case of contracts for the supply of products and services to be performed permanently or recurrently.”

→ art. 3, § 1, 3) Directive 2002/65/EC on financial services (FS-D)

“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning:

3) the distance contract (...)

(b) the minimum duration of the distance contract in the case of financial services to be performed permanently or recurrently;(…)”

4.4. Conclusion of the contract

4.4.1. Contract terms and general conditions

4.4.1.1. availability

This criterion concerns the availability of the contractual terms and conditions. It requires the merchant to:

- draft the terms and conditions in plain and intelligible language;
- ensure efficient accessibility.

The Code should stipulate that general terms and conditions must be made easily accessible, e.g., put on the homepage of the website in a sufficiently big letter type and readable, etc.

4.4.1.2. means to store and reproduce them

This criterion concerns the merchant's obligation to offer efficient technical means to store and reproduce the contractual terms and conditions.

→ art. 10, § 3 Directive 2000/31/EC on electronic commerce (EC-D)

“Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.”

→ art. 5 (Communication of the contractual terms and conditions and of the prior information) Directive 2002/65/EC on financial services (FS-D)

“1. The supplier shall communicate to the consumer all the contractual terms and conditions and the information referred to in Article 3(1) and Article 4 on paper or on another durable medium available and accessible to the consumer in good time before the consumer is bound by any distance contract or offer.

2. The supplier shall fulfil his obligation under paragraph 1 immediately after the conclusion of the contract, if the contract has been concluded at the consumer's request using a means of distance communication which does not enable providing the contractual terms and conditions and the information in conformity with paragraph 1.

3. At any time during the contractual relationship the consumer is entitled, at his request, to receive the contractual terms and conditions on paper. In addition, the consumer is entitled to change the means of distance communication used, unless this is incompatible with the contract concluded or the nature of the financial service provided."

→ Directive 93/13/EEC on unfair terms in consumer contracts (UT-D)

art. 5. In the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail. This rule on interpretation shall not apply in the context of the procedures laid down in Article 7.

See also Annex:

"(i) irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract."

→ section 4, § 4, pt. 3, ETR

"The terms and conditions of the contract must be easily accessible and put in plain and intelligible language. They must be printable by the consumer.

Terms and conditions should be presented in a clear and unambiguous fashion.

There must be an express acceptance of them by consumers prior to the purchase."

→ art. 5, §§ 1 and 2, GBDe (M)

§ 1. "As set out below, merchants shall:

- (...)
- **make available to consumers all relevant information relating to the terms and conditions, costs, shipping and charging and cancellation/return/refund policies applicable to a transaction before it is entered into; (...)."**

§ 2. "Merchants shall make available to consumers the terms and conditions applicable to the transaction. (...)."

4.4.2. Order procedure

This criterion concerns the difficult interaction between the electronic commerce Directive and article 5 of the Directive selling directive. One of the main consequences of this articulation is that some information must be given multiple times. For this reason, it can be that consumers do not know what they have to receive and when they should receive this information.

For this reason, we will pay attention to the fact that the code of conduct clearly describes the order procedure, the different steps one has to take to come to a legally binding act, and the obligations of the service provider.

4.4.2.1. Clear information

In view of the nature of the technology used and bearing in mind the need to enhance and ensure consumer confidence, the Directive on electronic commerce includes additional information obligations in relation to the technical aspects of the formation of the contract. With electronic commerce, technically new means to conclude contracts are becoming

available. In order to ensure that consumers can benefit from these opportunities, these new means of concluding contracts, with which they are not familiar, should be explained to them.

The information obligation on the conclusion of (electronic) contracts provides that the service provider must explain the manner of the formation of a contract by electronic means. This must be done clearly and unequivocally, prior to the conclusion of the contract, in such a way as to ensure that parties can give their full and informed consent.

→ art. 10, § 1, a) Directive 2000/31/EC on electronic commerce (EC-D)

***“1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:
(a) the different technical steps to follow to conclude the contract; (...).”***

4.4.2.2. Confirmation process

This criterion refers to a very specific stage of the contractual process that is not explicitly covered by hard law. Before placing the order, service providers or merchants should provide consumers with an opportunity to review the transaction and to confirm their intent to enter into the transaction. Prior to a transaction becoming a binding legal obligation, merchants should provide consumers with a summary that identifies precisely the goods or the services to be purchased, the terms and conditions of the transaction and the selected payment method.

→ section 4, § 5, ETR

***“Subscribers must ensure that, before placing the order, consumers can:
- review the goods/services to be purchased and the selected payment method;
- cancel the order;
- modify the order;
- express an informed and deliberate consent to the purchase;
- retain a complete and accurate record of the transaction.”***

→ art. 5, §§ 1 and 5, GBDe (M)

§ 1. ***“As set out below, merchants shall:***

- (...)
- ***provide consumers with an opportunity to review the transaction before it is completed and becomes a binding obligation; and (...).”***

§ 5. ***“Merchants shall provide consumers with an opportunity to review the transaction and to confirm their intent to enter into the transaction and shall disclose to consumers at what point the transaction will be final and become a binding obligation. Prior to a transaction becoming a binding obligation, merchants should provide consumers with a summary that includes:***

- ***the terms and conditions of the transaction;***
- ***the selected payment method; and***
- ***the option to cancel or affirmatively complete the transaction.”***

→ art. 2, § 5, e-Conf. Specific Guidelines

“Consumers, before placing the order, are able to review it, through a summary that identifies precisely the goods or services to be purchased and the selected payment method.

Consumers are able to modify their ordering intentions, express a deliberate consent to the purchase, terminate the purchase process before concluding the contract and retain a complete and accurate record of the transaction.”

4.4.2.3. Placing of the order (acknowledgement of receipt)

This criterion refers to the merchant’s obligation to acknowledge the receipt of the consumer’s order without undue delay and by electronic means.

Unlike the Commission’s initial proposal, the Directive on electronic commerce does not specify the time at which a contract would be deemed to be concluded. It only states that the provider has to acknowledge the receipt of the recipient’s order without undue delay and by electronic means. The order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

→ art. 11, § 1 Directive 2000/31/EC on electronic commerce (EC-D)

“1. Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:

- the service provider has to acknowledge the receipt of the recipient’s order without undue delay and by electronic means,**
- the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.”**

4.4.2.4. Written confirmation

→ art. 5 (Written confirmation of information) Directive 97/7/EC on distance contracts (DC-D)

“1. The consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information referred to in Article 4 (1) (a) to (f), in good time during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him.

In any event the following must be provided:

- written information on the conditions and procedures for exercising the right of withdrawal, within the meaning of Article 6, including the cases referred to in the first indent of Article 6 (3),**
- 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 conclusion for cancelling the contract, where it is of unspecified duration or a duration exceeding one year.**

2. Paragraph 1 shall not apply to services which are performed through the use of a means of distance communication, where they are supplied on only one occasion and are invoiced by the operator of the means of distance communication. Nevertheless, the consumer must in all cases be able to obtain the geographical address of the place of business of the supplier to which he may address any complaints.”

→ section 4, § 6 and § 4, pt. 4, ETR⁴¹

§ 6. “When acknowledging receipt of the order, subscribers must include a summary of the order. This summary should include:

- the date and time of order;
- a statement of what was ordered, the price, and any other charges;
- the method of payment and an indication of the earliest billing time;
- a unique purchase number;
- sufficient contact information to enable purchasers to obtain order status updates; and
- where applicable the anticipated date of dispatch.

§ 4, pt. 4. “Supplementary to all legally required information and other relevant information the subscriber must provide the following information:

- (...);
- Information to consumers that subscribers may reject orders should there be a reasonable suspicion that such orders may be fraudulent;
- (...).”

→ art. 5, § 6, GBDe (M)

“Merchants shall maintain, and make it possible for consumers to access, an appropriate record of information about a transaction for a reasonable period of time after it has been completed. Such information should include:

- a statement of what was ordered, the price, and any other known charges such as shipping/handling and taxes;
- sufficient contact information to enable purchasers to obtain order status updates; and
- the anticipated date of shipment.”

→ art. 3, § 2, e-Conf. Specific Guidelines

“A summary of the order is included when acknowledging receipt of the order. This summary should include:

- the date and time of order;
- a statement of what was ordered, the price, and any other charges;
- the method of payment and an indication of the moment when the code subscriber will initiate the debiting or charging process;
- a unique reference number;
- sufficient contact information to enable purchasers to obtain order status updates; and
- the anticipated date of shipment.

This recapitulation is sent when acknowledging the order within 24 hours of receipt of the order. When the goods or services have been dispatched, a record of dispatch and a confirmation that accounts have been debited is made available to the consumer.”

⁴¹ No agreement was reached on the following point; BEUC’s proposal: “This acknowledgement is sent as soon as possible, but at the latest within 2 working days of receipt of the order” and UNICE’s proposal: “The acknowledgement is sent without undue delay, e.g. within 2 working days of receipt of the order”.

4.4.3. Order error protections:

This criterion refers to a double obligation contained in the Directive on electronic commerce. The Directive includes the obligation for the service provider to make available to consumers appropriate means allowing them to identify and correct handling errors during the process of concluding a contract and also to provide information to consumers about the availability of such means. We, however, stress that this relates to the “technical” aspects to conclude a contract, not directly to the consent aspects.

4.4.3.1. Clear information

→ art. 10, § 1, a) Directive 2000/31/EC on electronic commerce (EC-D)

“1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service: (...) (c) the technical means for identifying and correcting input errors prior to the placing of the order; (...).”

4.4.3.2. Means to identify and correct handling errors

→ art. 11, § 2 Directive 2000/31/EC on electronic commerce (EC-D)

“Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.”

4.4.4. Cancellation/refund/return terms

This criterion covers the merchant’s obligations regarding the cancellation and refund modalities of the contract. It requires the following practice of the merchant:

- Information on the existence of a right of withdrawal and the conditions for exercising it;
- Information on the modes of refund;
- Information on the modes of dealing with unavailable goods, faulty goods and the goods not consistent with the agreed contractual terms.

4.4.4.1. Information on a right of withdrawal

Information should be given on the conditions and situations for exercising one’s right of withdrawal. Furthermore, it is important that consumers receive transparent information on how they can exercise this right.

→ Directive 97/7/EC on distance contracts (DC-D)

art. 4, § 1 (see also art. 5). “1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (...) (f) the existence of a right of withdrawal, except in the cases referred to in Article 6 (3); rate; (...).”

art. 6 (Right of withdrawal).

“1. For any distance contract the consumer shall have a period of at least seven working days in which to withdraw from the contract without penalty and without giving any reason. The only charge that may be made to the consumer because of the exercise of his right of withdrawal is the direct cost of returning the goods.

The period for exercise of this right shall begin:

- **in the case of goods, from the day of receipt by the consumer where the obligations laid down in Article 5 have been fulfilled,**
- **in the case of services, from the day of conclusion of the contract or from the day on which the obligations laid down in Article 5 were fulfilled if they are fulfilled after conclusion of the contract, provided that this period does not exceed the three-month period referred to in the following subparagraph.**

If the supplier has failed to fulfil the obligations laid down in Article 5, the period shall be three months. The period shall begin:

- **in the case of goods, from the day of receipt by the consumer,**
- **in the case of services, from the day of conclusion of the contract.**

If the information referred to in Article 5 is supplied within this three-month period, the seven working day period referred to in the first subparagraph shall begin as from that moment.

2. Where the right of withdrawal has been exercised by the consumer pursuant to this Article, the supplier shall be obliged to reimburse the sums paid by the consumer free of charge. The only charge that may be made to the consumer because of the exercise of his right of withdrawal is the direct cost of returning the goods. Such reimbursement must be carried out as soon as possible and in any case within 30 days. (...).”

→ Directive 2002/65/EC on financial services (FS-D)

art. 3, § 1, 3). “1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning: (...)

3) the distance contract

(a) the existence or absence of a right of withdrawal in accordance with Article 6 and, where the right of withdrawal exists, its duration and the conditions for exercising it, including information on the amount which the consumer may be required to pay on the basis of Article 7(1), as well as the consequences of non-exercise of that right;

d) practical instructions for exercising the right of withdrawal indicating, inter alia, the address to which the notification of a withdrawal should be sent; (...).”

+ art. 6 and art. 7.

→ Recommendation 92/295/EEC on codes of practice for the protection of consumers in respect of contracts negotiated at distance (distance selling) (CP-Rec)

See Annex “Points which could be covered by codes of practice for contracts negotiated at a distance”: “(...)

- **Right of withdrawal: if the consumer chooses to make use of the right of withdrawal, a period within which payments already made will be reimbursed.”**

→ section 4, § 4, pt. 4, ETR

“Supplementary to all legally required information and other relevant information the subscriber must provide the following information:

- (...);
- **Information on the existence or non-existence of the right of withdrawal and period, if any; (...).”**

→ art. 5, § 2, al. 2, GBDe (M)

“For ongoing transactions or subscriptions:

- (...)
- **minimum duration of the contract and easy-to-understand cancellation information, an easy to use means to cancel an ongoing subscription, and timely confirmation of such cancellation.”**

4.4.4.2. Information on refund modes

Information should be given on the conditions and situations for exercising one's right of refund. Furthermore, it is important that consumers receive transparent information on how they can exercise this right. Codes of Conduct can, for instance, specify the modes of dealing with faulty goods and the goods not consistent with the agreed contractual conditions (faulty goods).

→ Directive 1999/44/EC on the sale of consumer goods and associated guarantees (GG-D)

art. 3, § 1. “The seller shall be liable to the consumer for any lack of conformity which exists at the time the goods were delivered.”

art. 9. “Member States shall take appropriate measures to inform the consumer of the national law transposing this Directive and shall encourage, where appropriate, professional organisations to inform consumers of their rights.”

→ art. 3, § 1, 3) Directive 2002/65/EC on financial services (FS-D)

“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning:

3) the distance contract (...)

(c) information on any rights the parties may have to terminate the contract early or unilaterally by virtue of the terms of the distance contract, including any penalties imposed by the contract in such cases;(…).”

→ section 4, § 4, pt. 4, ETR

“Supplementary to all legally required information and other relevant information the subscriber must provide the following information:

- (...);
- **Information about the return policy including any costs of return;**
- (...).”

→ art. 6, § 1, GBDe (M)

“Merchants shall provide information to consumers about their cancellation, return, and refund policies, including: the length of time after entering into a binding obligation which an available

cancellation, return, or refund may be made; the process that should be followed; and any costs that may be incurred. If there is no cancellation, return or refund right, this should be stated.”

4.4.5. Payment

This criterion concerns the service provider’s obligations regarding payment. It requires the following practice of the service provider or merchant:

- Clear information on the different accepted payment methods;
- Use of payment methods that are easy and less expensive for customers.

→ art. 4, § 1 Directive 97/7/EC on distance contracts (DC-D)

**“1. In good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information: (...)
(e) the arrangements for payment, delivery or performance; (...).”**

→ art. 3, § 1, 2), f Directive 2002/65/EC on financial services (FS-D)

**“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning: (...)
2) the financial service
(f) the arrangements for payment and for performance; (...).”**

→ art. 8 (Payment by card) Directive 97/7/EC on distance contracts (DC-D) and Directive 2002/65/EC on financial services (FS-D)⁴²

→ section 4, § 4, pt. 4, ETR

**“Supplementary to all legally required information and other relevant information the subscriber must provide the following information:
- Information about the types of payment that will be accepted and the implications of each in terms of any extra charges or discounts as well as the earliest billing time;
- (...).”**

→ art. 5, § 2, al. 1 and 2, GBDe (M)

al. 1. “Merchants shall make available to consumers the terms and conditions applicable to the transaction. Such information should include:

- (...)
- **easy-to-use payment mechanisms and in the case of credit or debit cards, the expected time when the card will be charged; (...).”**

al. 2. “For ongoing transactions or subscriptions:

⁴² See also Commission Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder; Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions; Directive 2000/28/EC of the European Parliament and of the Council of 18 September 2000 amending Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions; Regulation (EC) No 2560/2001 of the European Parliament and of the Council of 19 December 2001 on cross-border payments in euro

• information about how the transaction will appear on the bill so that the customer will be able to determine to which transaction and which company the bill relates; (...)."

→ See art. 2, § 3, al. 2, e-Conf. Specific guidelines

"Consumers are informed about the types of payment that will be accepted, the moment when the code subscriber will initiate the debiting or charging process and, as far as possible, the implications of each in terms of any extra charges or discounts."

We underline that no agreement was reached as to the billing process: the original BEUC proposal states that: "Except in the case of personalised goods/services, subscribers do not initiate the billing process until the good or service has been dispatched, unless the consumer has expressly agreed". UNICE's proposal holds that : "*there is no justification for this requirement. It is not present in any existing code or in any EU relevant rule and is not common practice. This method of payment would be overly burdensome on industry, in particular on SMEs. UNICE thinks that consumers are adequately protected by other requirements of the scheme (i.e. refund policy)*". Therefore, we do not consider this specific issue a relevant criterion for the benchmark list.

4.4.6. Inertia selling/unsolicited services

→ art. 9 (inertia selling) Directive 97/7/EC on distance contracts (DC-D)

"Member States shall take the measures necessary to:

- prohibit the supply of goods or services to a consumer without their being ordered by the consumer beforehand, where such supply involves a demand for payment,**
- exempt the consumer from the provision of any consideration in cases of unsolicited supply, the absence of a response not constituting consent."**

→ art. 9 (Unsolicited services) Directive 2002/65/EC on financial services (FS-D)

4.4.7. Filing of the contract

As we can observe, the Directive on electronic commerce only imposes on the service provider the obligation to indicate to consumers whether or not the concluded contract is filed and whether it is accessible. We note that the Directive does not impose an obligation to archive, but only an obligation to inform whether the contract is archived.

In our view, this requirement should be necessarily complemented with a positive obligation to put in place efficient storage mechanisms and to make the filed contract accessible to the customer in an easily readable manner.

4.4.7.1. Clear information

4.4.7.2. Accessibility

→ art. 10, § 1, b) Directive 2000/31/EC on electronic commerce (EC-D)

“1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service: (...) (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible; (...).”

→ section 4, § 5, ETR

“Subscribers must ensure that, before placing the order, consumers can:

- (...)
- ***retain a complete and accurate record of the transaction.”***

→ art. 5, §§ 1 and 6, GBDe (M)

§ 1. “As set out below, merchants shall:

- (...)
- ***maintain a record of the transaction after it has been completed.”***

§ 6. “Merchants shall maintain, and make it possible for consumers to access, an appropriate record of information about a transaction for a reasonable period of time after it has been completed. Such information should include:

- ***a statement of what was ordered, the price, and any other known charges such as shipping/handling and taxes;***
- ***sufficient contact information to enable purchasers to obtain order status updates; and***
- ***the anticipated date of shipment.”***

4.5. Customer service

The object of this criterion is the management of the customer service. It aims to require of the merchant that:

- In his business model there is a customer service;
- Although we are aware that not all TMS Members, notably SMEs, have the financial and human resources to create and maintain such a service, a specific consumer contact point is made available, if necessary in co-operation with other parties;
- He discloses information relating to this service; e.g. that he specifies the name of the person responsible for the customer service, his address, telephone number, etc.

It should be emphasized that the information on customer service for consumers must be clear, before talking about alternative dispute resolution (ADR) and complaint procedures. These aspects of dispute resolution are dealt with later. However, we refer already to them because a customer service can be the first point to start a complaint (in-house settlement or ADR).

4.5.1. Information about customer service & contact point

These services can be either general, e.g., contact point, or customer specific, notably a dedicated customer service.

It is important to make a distinction between a general customer service, directed at helping the customer in general, and a complaint entry. In the latter situation, the back office of the service provider shall be contacted with a specific aim, i.e., complaint entry and complaint handling. We underline that customer service can be the first entry of a complaint or first step in a dispute-resolution procedure.

→ art. 5, § 1 Directive 97/7/EC on distance contracts (DC-D)

“1. The consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information referred to in Article 4 (1) (a) to (f), in good time during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him.

In any event the following must be provided: (...)

- information on after-sales services and guarantees which exist, (...).

→ art. 8, §§ 1 and 2, GBDe (M)

§ 1. “Merchants shall comply with all commitments, representations, and other promises made to consumers. They shall disclose to consumers information regarding customer service and/or support of the goods and services that consumers purchase online. Such information should include the length of time the customer service and/or support is available, the costs associated with obtaining the customer service and/or support, and how customers can successfully and meaningfully contact the business to get answers to their questions.”

§ 2. “If no customer service and/or support are available from the merchant, this should be stated.”

4.5.2. Complaint procedure

The object of this criterion concerns the internal procedures for dealing with consumer complaints. In this respect, the merchant should:

- specify whether the company has put in place internal claim procedures and the terms of such procedures (time scale, costs, ...);
- operate in a way which provides adequate procedural guarantees for the concerned parties (principles of fairness, effectiveness, transparency, ...).

4.5.2.1. Clear information

→ art. 5, § 1 Directive 97/7/EC on distance contracts (DC-D)

“1. The consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information referred to in Article 4 (1) (a) to (f), in good time during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him.

In any event the following must be provided: (...)

- the geographical address of the place of business to which the consumer may address any complaints, (...).”

4.5.2.2. Principles

In order to ensure the quality of a complaint procedure, codes should impose certain principles upon their members.

Information should be given regarding the fairness, effectiveness, transparency and confidentiality of the procedure. Furthermore, one must also consider the delays in answering a complaint, guarantees in relation to corrective actions and their follow-up, responsible persons, written character of the procedure, etc.

→ section 4, § 10, al. 1, ETR

“Subscribers must have in place on-line access to an in-house complaint system, which is fair, effective, transparent and confidential. Complaints must be acknowledged within a short period of time and the consumer must be advised on the timescale for dealing with the complaint. The subscriber maintains a record of the complaints received and reports to the trustmark owner on them.”

→ art. 12, §§ 1 and 2, GBDe (M)

§ 1. “Merchants shall provide consumers with fair, timely, and affordable means to settle disputes and obtain redress.”

§ 2. “Merchants should provide an easy-to-find and understandable notice on how a consumer can successfully and meaningfully contact the merchant to solve problems related to a transaction. They should have effective ‘customer satisfaction systems’, encourage consumers to take advantage of such internal mechanisms and make a good faith effort to resolve any disputes relating to a transaction in a fair and equitable manner, for example, by providing money-back satisfaction guarantees or exchange policies. Complaints should be directed in the first instance to the merchant.”

→ art. 8, al. 1, e-Conf. General Principles

“Codes should require that code subscribers ensure their in-house complaint process is transparent, confidential, free to the consumer, easily accessible and responsive to complaints. The code-subscriber should respond to any complaint in a timely, clear and fair way with the aim of satisfying complainants and providing appropriate remedies.”

→ art. 5, § 1, e-Conf. Specific guidelines

“Code subscribers' own complaint handling ensures that:

- Consumers are given a contact point and information on how to lodge complaints;

- **Complaints are acknowledged and a reference given;**
- **Code-subscribers seek to resolve complaints within a reasonable period and if the consumer remains dissatisfied, provide information on the out of court settlement body it adheres to.**
- **Complaints are recorded and monitored and internal complaints handling is regularly reviewed.**

4.5.3. Information on alternative dispute resolution

This criterion concerns the “external phase” of the complaint procedure with an independent third party. The merchant should inform the parties on the alternative dispute-resolution scheme that he adheres to.

→ art. 17 (out-of-court dispute settlement) Directive 2000/31/EC on electronic commerce (EC-D)

“1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.

2. Member States shall 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.

3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce.”

→ art. 3, § 1, 4) Directive 2002/65/EC on financial services (FS-D)⁴³

“1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning: (...)

4) redress

(a) whether or not there is an out-of-court complaint and redress mechanism for the consumer that is party to the distance contract and, if so, the methods for having access to it; (...).”

→ Recommendation 2001/310/EC on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes (ADR-Rec1)

See pt. B (Transparency):

“1. The transparency of the procedure should be guaranteed.

2. Information about the contact details, functioning and availability of the procedure should be readily available to the parties in simple terms so that they can access and retain it before submitting a dispute. (...).”

→ Recommendation 98/257/EC on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes (ADR-Rec2)

⁴³ See also article 14 (Out-of-court redress)

“1. Member States shall promote the setting up or development of adequate and effective out-of-court complaints and redress procedures for the settlement of consumer disputes concerning financial services provided at distance.

2. Member States shall, in particular, encourage the bodies responsible for out-of-court settlement of disputes to co-operate in the resolution of cross-border disputes concerning financial services provided at a distance.”

→ section 4, § 4, pt. 4 and § 10, al. 2, ETR

§ 4, pt. 4. *“Supplementary to all legally required information and other relevant information the subscriber must provide the following information:*

- (...);

- Information about the identity of the alternative dispute-resolution scheme to which the subscriber adheres (including a link to any relevant website); (...).”

§ 10, al. 2. *“When the consumer remains dissatisfied, the subscriber should provide information on the alternative dispute-resolution scheme that he adheres to.”*

→ art. 12, §§ 3 to 6, GBDe (M)

§ 3. *“Unless full customer satisfaction is guaranteed by an internal customer satisfaction system, merchants should notify consumers that they are ready to submit disputes resulting from a transaction to one or more specified ADR systems. Information about the ADR offered should be provided as a part of the notice on how consumers can contact the merchant to resolve problems related to a transaction and access to an ADR system normally should be available only after a consumer has sought redress through a merchant’s internal complaints mechanism.”*

§ 4. *“Such ADR systems would not affect the consumer’s right to seek remedies through the court system. However, the consumer and the merchant could agree that prior to proceeding in the court of any local jurisdiction, the consumer would submit a claim to an ADR system. ADR systems should function according to published rules of procedure that describe unambiguously all relevant elements necessary to enable consumers seeking redress to take fully informed decisions on whether they wish to use the ADR offered or to address themselves to a court of law.”*

§ 5. *ADR systems should provide for impartial, accessible, transparent, and timely conciliation/negotiation, mediation and/or arbitration at no or only moderate cost for the consumer.”*

§ 6. *“Consumers should be informed about the conditions of access (online or other), the cost, the legal nature of the ADR (arbitration, mediation, conciliation/negotiation, etc.) and of its outcome (binding/not binding/binding for the merchant; enforceable), and recourse to other instances, notably to law courts.”*

→ art. 8, al. 2, e-Conf. General Principles

“Where the in-house complaint process fails to satisfy a complainant, the Code should require that Code subscribers agree to submit that dispute to an out of court settlement body that meets the requirements of the Commission Recommendations on out -of-court settlement bodies and accept the outcome.”

→ art. 5, §§ 1 and 2, e-Conf. Specific Guidelines

§ 1. *“Code subscribers’ own complaint handling ensures that:*

- (...)

- Code-subscribers seek to resolve complaints within a reasonable period and if the consumer remains dissatisfied, provide information on the out of court settlement body it adheres to.
(...).”

§ 2. *“In the event that recourse is had to an out-of-court settlement body, code subscribers inform code owners of the outcome of the dispute resolution process.”*

4.6. Commercial communications and fair marketing practices

This criterion deals with the different modes of advertising and marketing practices (particular attention should be paid to on-line advertising). These rules are governed by several fundamental principles:

- **Principle of transparency and identification:** clear identification of the commercial communication, the advertiser and promotional offers and promotional competitions or games.
- **Principle of fair trading:** one of the main objectives of rules on advertising is to protect consumers against misleading advertising and the unfair consequences thereof.
- **Principle of intimacy:** problems of unsolicited commercial communications. Consumer's right of privacy, particularly as regards freedom from certain particularly intrusive means of communication should be recognized.

4.6.1. Commercial communications

→ art. 6 Directive 2000/31/EC on electronic commerce (EC-D)

“In addition to other information requirements established by Community law, Member States shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions:

(a) the commercial communication shall be clearly identifiable as such;

(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;

(c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;

(d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.”

→ art. 7, §§ 4-5 Proposal for a Directive concerning unfair business-to-consumer commercial practices in the Internal Market (UCP-Prop D)

§ 4. “Information requirements in relation to advertising, commercial communication or marketing established by Community law shall be regarded as material.”

§ 5. “Annex 2 contains a non-exhaustive list of Community law provisions setting out information requirements in relation to commercial communication, advertising or marketing.”

4.6.2. Fair marketing practices

Given the broad framework for advertising and fair marketing practises, and the fields it encompasses, this topic should be reviewed in a broad and general manner.

→ Directive 97/55/EC amending Directive 84/450/EEC concerning misleading advertising so as to include comparative advertising (MA-D)

→ Directive 84/450/EEC concerning misleading advertising so as to include comparative advertising (MA-D)

→ Proposal for a Directive of 17 June 2003 concerning unfair business-to-consumer commercial practices in the Internal Market (UCP-Prop D)

→ Recommendation 92/295/EEC on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling) (CP-Rec)

See Annex "Points which could be covered by codes of practice for contracts negotiated at a distance": "(...)

- *Sales promotion: provisions covering sales promotion techniques (reduction, rebates, gifts, lotteries and competitions) to ensure that the principles of fair competition are respected and in particular that the consumer receives clear information, (...).*"

→ section 4, § 2, ETR

"Subscribers must ensure that all commercial communications are fair and in accordance with good marketing practices as defined, for example, by industry self-regulatory programs.

Subscribers should be able to substantiate any express or reasonably implied factual claims made in their advertising or marketing and should possess reasonable substantiation prior to disseminating a claim.

Information about the basis for any price comparisons should be readily available and regularly updated by subscribers.

Subscribers should not knowingly link to, or accept, affinity or royalty payments from fraudulent or illegal sites.

Subscribers should make the complete rules for any offered contests, sweepstakes or games easily available online.

Subscribers should take into account the regulatory characteristics of the markets they target.

Subscribers should not use Internet technology to mislead consumers about the nature of the product or service being promoted or offered.

Subscribers should ensure that search terms fairly reflect the content of the site."

→ art. 1, § 2 and 2, § 1, GBDe (M)

art. 1, § 2. *"Merchants shall not make any representation or omission or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair to consumers.*

art. 2, § 1. *"Merchants should take the necessary steps to ensure that any representation about a good or service is current, accurate, and not deceptive or misleading to consumers and that the truthfulness of objective claims be substantiated."*

→ art. 1, § 1 and § 2, al. 1, e-Conf. Specific Guidelines

§ 1. “Participation by code subscribers in industry self-regulatory advertising programmes is encouraged.

Any reasonably implied claims made in advertising or marketing by code subscribers possess reasonable substantiation. This should be available prior to disseminating a claim.

Information about the basis for any price comparisons is readily available and regularly updated by code subscribers.

Consumers are able to access the complete rules for any offered contests, sweepstakes or other similar promotions.

§ 2, al. 1. Internet technology should be used to promote the consumer’s knowledge of the products or services being offered and should not mislead. For example, hyperlinks should not be used to contradict or substantially change the meaning of any material statement or claims.”

4.6.3. Unsolicited commercial communications

We underline that this criterion does not only relate to the sending of traditional email, but that the OPT-IN principle is also applicable to other kinds of commercial communications such as e-cards, newsletters and pop-up windows.

In relation to the latter kind of messages, we underline that article 2(h) of Directive 2002/58/EC states that electronic mail, subject of the OPT-IN regime, is any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

In other words, any message that is i) stored in a network or in the recipient's terminal equipment and ii) is collected by the recipient, should be considered electronic mail.

- As to the first requirement, a pop-up window is not only stored in the network, e.g., on the http server of the pop-up window sender, but is also stored in the terminal equipment of the recipient. In absence of any reference in this regard, all storage in the terminal equipment must be considered, even when only for a few milliseconds. Before a pop-up window can be displayed on one’s computer screen, it needs to be stored in the RAM memory of the video card, i.e., a part of the recipients terminal equipment.
- As to the second requirement, one could defend that a pop-up message is collected by the recipient, merely by connecting his terminal equipment, i.e., client side, with the server concerned. Indeed, it would be difficult to defend that a hotmail address is not considered an electronic mail address. However, unlike the more traditional inboxes, using the POP, IMAP or SMTP protocol, a hotmail “inbox” must be considered a private HTTP web page. From a technical and functional point of view, there is not much difference between the functioning of a pop-window and the display of your “inbox” on www.hotmail.com. One of the only differences is that access to the latter page is subject to giving the corresponding personal login and password, often stored on a cookie or similar device.

In conclusion, we shall also consider whether the spam problem in relation to chat boxes and online forums is considered.

→ art. 13 Directive 2002/58/EC on privacy and telecommunications (PT-D)

“1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.”

→ art. 7 Directive 2000/31/EC on electronic commerce (EC-D)

“1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.

2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.”

→ art. 10 Directive 97/7/EC on distance contracts (DC-D)

Restrictions on the use of certain means of distance communication

1. Use by a supplier of the following means requires the prior consent of the consumer:

- automated calling system without human intervention (automatic calling machine),
- facsimile machine (fax).

2. Member States shall ensure that means of distance communication, other than those referred to in paragraph 1, which allow individual communications may be used only where there is no clear objection from the consumer.

→ art. 10 Directive 2002/65/EC on financial services (FS-D)

→ art. 11, §§ 1 to 3, GBDe (M)

§ 1. “Merchants shall accurately describe their business practices with regard to their use of unsolicited e-mail to consumers.”

§ 2. “Merchants that engage in unsolicited email marketing should adhere to a policy that, at a minimum, enables those consumers who do not wish to be contacted online to opt out online from future solicitations. This policy should be available both on the web site and in any e-mails, other than those relating to a particular order.”

§ 3. “Merchants that engage in unsolicited email marketing should also subscribe to a bona-fide e-mail suppression list.”

4.7. Security of system and payment

This criterion concerns the security issues related to the merchant’s website, including the payment mechanisms. Those responsible for the website should:

- make reference to the security standards (security policy) and identify a person responsible for the security of the website (contact point);
- use technical solutions to ensure the security of the website, payment and transactions, the personal data processed and the confidentiality of the communications exchanged with parties.

For electronic commerce, even more than for other forms of commerce, payment and rules are crucial elements for establishing and enhancing consumers’ confidence. . As regards payment as such, there is no specific European community consumer protection legislation (except the requirements regarding information on payment methods⁴⁴).

4.7.1. Information on security policy and contact point

Website visitors, both consumers and businesses, should find information and references about the implemented security standards and adopted security policy.

→ section 4, § 4, pt. 4, ETR

“Supplementary to all legally required information and other relevant information the subscriber must provide the following information:

- (...);
- **Information about the security and authentication systems the subscriber uses to enable consumers to assess the risk in relying on these systems;**
- (...).”

→ art. ?, al. 3 and 4, e-Conf. Specific Guidelines

“Consumers are informed of the technology used to protect the transmission of financial information.

Information critical to establishing confidence, and in particular trustmarks and webseals, are authenticated using effective technical mechanisms.”

⁴⁴ Some Directives or other initiatives do, however, contain relevant provisions.

4.7.2. Implementation of technical requirements

→ art. 16 (Confidentiality of processing) and 17 (Security of processing) 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 (DP-D)

art. 16. “Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.”

Art. 17. “1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- **the processor shall act only on instructions from the controller,**
- **the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.**

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.”

→ art. 4 (Security) and art. 5 (Confidentiality of the communications) Directive 2002/58/EC on privacy and telecommunications (PT-D)

art. 4. “1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.”

art. 5. “1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).

This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.”

→ Directive 1999/93/EC on a Community framework for electronic signatures

→ Recommendation 97/489/EC concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder

→ section 4, § 8, ETR

Security of system

“Subscribers must have an effective security policy to keep consumers personal and transactional information confidential and to prevent it from being interfered with. This security policy should be regularly reviewed.

Any subcontractors or third parties involved in the operation of the website or its transactions must also have an effective security policy.

Steps must be taken to prevent the content of the site from being interfered with.

Subscribers must provide general information about the level of security being used on their site and identify a contact point responsible for security.”

Security of payment

High-standard technological means should be used to ensure the authenticity and confidentiality of financial transactions and payments made by consumers.

Subscribers must provide general information on the technology used to protect the transmission of financial information.”

→ art. 7, § 1, GBDe (M)

“For information that is transferred from a consumer to a merchant, merchants shall take reasonable steps ensure the security of a consumer’s confidential commercial and personal information. These security efforts shall be consistent with best industry practices and shall be appropriate for the type of information collected, maintained or transferred to third parties. In particular, merchants should:

- **have in place encryption measures that reflect best industry practices for the transfer or receipt of sensitive information, such as personal financial information or health care records;**
- **have in place appropriate levels of security to protect data being maintained by computers;**
- **take reasonable steps to require third parties involved in fulfilling a customer transaction to also maintain appropriate levels of security; and**
- **not retain any information from which a consumer may be identified if the consumer does not complete a transaction, without the consumer’s consent.”**

→ art. 9, al. 1, e-Conf. General Principles

“Codes should require code-subscribers (and any third parties involved in fulfilment of a transaction) to adopt best practices for ensuring the integrity and confidentiality of transactions and assuring consumers of the authenticity of the information supplied by the code-subscriber. Codes should require that code subscribers regularly review the security of their technology and their security practices and use the best available technology that does not incur excessive costs for them or for the consumer. Codes should require that code subscribers do not contract out of responsibility for losses arising from the misuse or failure of authentication mechanisms.”

→ See art. ?, al. 1 and 2, e-Conf. Specific Guidelines

“Technological means are used to ensure the authenticity and confidentiality of financial transactions and payments.

In-house security systems are established to safeguard the integrity and confidentiality of transactions and payments made by consumers.”

4.8. Personal-data protection

This criterion deals with personal-data protection. As a data controller, the merchant should:

- Make reference to a privacy policy in an clear and intelligible way (hyperlink on homepage to the privacy policy) and appoint a person responsible for privacy-related aspects;
- Provide information (minimum) on the identity of the controller, the purpose of the process, the recipients of the process and the right of access and rectification.
- Notify his national Data Protection Authority.

4.8.1. Reference to privacy policy

→ art. 27 (Codes of conduct) 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 (DP-D)

“1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.”

→ section 4, § 4, pt. 4, ETR

“Supplementary to all legally required information and other relevant information the subscriber must provide the following information:

- (...);
- **The subscriber’s privacy policy.”**

4.8.2. Information

4.8.2.1. Identity of the controller

4.8.2.2. Purpose of the process

Information should be provided on the reasons of data collection and processing, in particular when cookies and other tracking technology is used.

4.8.2.3. Recipients

4.8.2.4. Right of access and rectification

→ 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 (DP-D)

→ Directive 2002/58/EC on privacy and telecommunications (PT-D)

art. 4 (Security)

art. 5 (Confidentiality of the communications)

art. 9 (Location data other than traffic data)

→ section 4, § 9, al. 1 and 3, ETR

al. 1. **“A contact point responsible for privacy inquiries must be clearly indicated. A statement summarising the subscriber’s privacy policy should be made easily available before or at any time when data is collected. It must include information on:**

- **what information is being collected;**
- **how it is collected;**
- **who is collecting;**
- **what the information is to be used for;**
- **the use, if any, of cookies/tracking technologies and their purpose.**

al. 3. **“The use of privacy-enhancing technologies is encouraged and information to consumers about them should be provided.”**

→ art. 10, §§ 1 and 2, GBDe (M)

§ 1. **“Merchants shall post and adhere to a privacy policy that is open, transparent, and consistent with the following personal data protection practices:**

- **Notice /Awareness: Merchants that collect personal data shall reasonably explain what personal data they collect, use, and disclose to third parties, and for what purposes;**
- **Choice/Consent: Merchants that collect personal data shall reasonably explain what choices they provide consumers about the collection, use and disclosure of such information. At a minimum, Merchants should provide consumers with the choice to opt out of having their personal data used or disclosed for any new purpose not explained at the time the personal data was collected and should obtain the consumer’s unambiguous consent to the collection or use of sensitive personal information, such as medical records.**

- **Accuracy:** Merchants that collect personal data shall reasonably explain the methods by which the consumer can correct or update personal data and shall adopt procedures to respond to reasonable consumers' requests for such corrections or updates.
- **Integrity/Security:** Merchants that collect personal data shall reasonably explain the steps taken to protect the quality and integrity of the personal data collected as well as the confidentiality of that personal data from unauthorized access.
- **Redress/Internal Rules:** Merchants shall reasonably explain the means of communicating with the merchant's contact point to which the consumer can direct questions, express preferences concerning the handling of personal data or lodge complaints. Merchants shall establish and maintain a system to implement the provisions of these guidelines within the company."

§ 2. "When transferring personal data to a third party for processing on its behalf, a merchant should ascertain the adequacy of the personal data practices of the third party"

→ art. 10, e-Conf. General Principles

"Codes should require code subscribers to make a summary of their data protection policy publicly available, in particular on-line. Code-owners and code subscribers should take advantage of the opportunities set out under Article 27 of the Data Protection Directive 95/46/EC for national or EU approval of data protection codes of conduct either:

- to adhere to a code of conduct on data protection that has been approved;
- or submit the parts of the e-commerce code itself that cover data protection for approval."

→ art. 4, al. 1 and 2, e-Conf. Specific Guidelines

al. 1. "The summary of code subscribers' data protection policies provides information on the practices observed to ensure compliance with the provisions of the European Union's data protection directives. The summary should also provide the following information:

- A contact point for inquiries
- The use, if any, of cookies or tracking technology and their purpose"

al. 2. "The use of privacy enhancing technologies is encouraged and information to consumers about them is provided."

4.8.3. Notification to national DPA

4.9. Protection of children

More and more under-aged people become the object of providers of information society services. Even though minors cannot legally conclude contracts, they *de facto* participate in, and benefit from, in the Information Society. Considering this particular context and to protect the vulnerable, some specific questions need to be answered. In some Member States, national Data Protection Authorities (DPA)⁴⁵ have adopted (non-binding) opinions regarding new technologies and the protection of minors. In France⁴⁶ and Belgium⁴⁷, public advisory bodies have supported these initiatives and published advice in this regard. However, in

⁴⁵ See for instance the opinion of the Belgian DPA on the online protection of minors. Commissie voor de bescherming van de persoonlijke levenssfeer, Advies uit eigen beweging betreffende de bescherming van de persoonlijke levenssfeer van minderjarigen op Internet, 16 September 2002. www.privacy.fgov.be

⁴⁶ Forum des droits sur l'internet, Recommandation 'Les Enfants du Net - (1) Les mineurs et les contenus préjudiciables sur l'internet', 11 February 2004, <http://www.foruminternet.org/recommandations/lire.phtml?id=694>

⁴⁷ l'Observatoire des Droits de l'Internet, Avis n° 1 sur la protection des mineurs sur l'internet, 29 January 2003, http://www.internet-observatory.be/internet_observatory/pdf/advices/advice_fr_001.pdf

absence of particular positive legal obligations regarding the online protection of minors, we believe that soft law could make a valuable contribution in this area.

In this view, we will consider whether codes of conduct promote parental consent, encourage children to buy, provide information on safety guidelines, labelling and filtering technologies, etc.

→ art. 16, § 1 Directive 2000/31/EC on electronic commerce (EC-D)

***“1. Member States and the Commission shall encourage: (...)
(e) the drawing up of codes of conduct regarding the protection of minors and human dignity.”***

→ art. 2, § 2, GBDe

“If marketing or other online activities are directed at children, or where the website knows the visitor is a child, merchants shall take special care to protect children by recognizing their vulnerabilities. (...)”

→ art. 1, al. 3, e-Conf. General Principles

“(...). Codes should pay particular attention to the potential vulnerability of certain consumers such as minors, the elderly and the seriously ill.

4.9.1. Commercial communications and fair marketing practices

→ art. 4, § 2 Directive 97/7/EC on distance contracts (DC-D)

“The information referred to in paragraph 1, the commercial purpose of which must be made clear, shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions, and the principles governing the protection of those who are unable, pursuant to the legislation of the Member States, to give their consent, such as minors.”

→ Proposal for a Directive concerning unfair business-to-consumer commercial practices in the Internal Market (UCP-Prop D)

See Annex 1 (Commercial practices, which are in all circumstances considered unfair)

“Aggressive commercial practices (...)

(6) Advertising to children in a way which implies that their acceptance by their peers is dependent on their parents buying them a particular product. This provision is without prejudice to Article 16 of Directive 89/552/EEC on television broadcasting.”

→ Recommendation 98/560/EC on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (M-Rec)

“II. RECOMMENDS that the industries and parties concerned:

(2) co-operate in the drawing up of codes of conduct for the protection of minors and human dignity applying to the provision of on-line services, inter alia to create an environment favourable to the development of new services, taking into account the principles and the methodology described in the Annex; Member States and parties concerned in the various fields covered by this recommendation; (...).”

See also Annex “Indicative guidelines for the implementation, at national level, of a self-regulation framework for the protection of minors and human dignity in on-line audiovisual and information services”, pt. 2.2.1.

→ Decision N° 276/1999/EC of 25 January 1999 ‘adopting a multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (IHC-De)

→ section 4, § 3, ETR

“Subscribers must ensure that commercial communications, advertising or promotional activities

- *take into account the age, knowledge and level of maturity of the intended audience and identify material intended only for adults,*
- *do not encourage children to enter inappropriate websites;*

Subscribers must ensure that websites addressing children:

- *do not cause moral, mental or physical detriment to children,*
- *encourage children to gain parental consent prior to on-line purchasing,*
- *do not encourage children to contract for credit or engage in long-term contracts,*
- *do not encourage children to buy a product or a service by exploiting their inexperience, sense of loyalty, credulity or trust,*
- *do not lead children to persuade their parents or others to purchase the goods or services on offer,*
- *make guidelines for safe shopping for children available.”*

→ art. 1, § 2, al. 2 and § 3 and art. 2, § 4, e-Conf. Specific Guidelines

art. 1, § 2, al. 2. ***“Tools and practices that facilitate searching, the seeking of parental consent by children and the monitoring by parents of children’s use of the Internet should be encouraged.”***

art. 1, § 3. ***“Commercial communications:***

- *do not cause moral, mental or physical detriment to children,*
- *take into account the age, knowledge and level of maturity of the intended audience and identify material intended only for adults:*
- *do not encourage children to buy a product or a service by exploiting their inexperience, sense of loyalty, natural credulity or the special trust children place in parents or other persons;*
- *do not encourage children to enter inappropriate websites nor to communicate with inappropriate persons;*
- *do not encourage children to contract for the sale or rental of goods and services or for credit without parental consent.”*

art. 2, § 4. ***“Children are encouraged to gain parental consent before making any commitment to purchase a good or a service.***

Children are not be encouraged to contract for credit.”

4.9.2. Harmful content

4.9.3. Personal-data protection

→ 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 (DP-D)

→ Directive 2002/58/EC on privacy and telecommunications (PT-D)

→ section 4, § 9, al. 2, ETR

“In addition to legal requirements, subscribers must take special care with data collected from children, as follows:

- Awareness tools to encourage children to obtain permission from parents should be used;
- Parental permission for the collection of data must be sought.”

→ art. 2, § 2, GBDe (M)

“(…). In particular, a merchant shall seek to ensure parental permission is obtained before collecting, using or disclosing the child’s personal data or completing a transaction.”

→ art. 4, al. 3, e-Conf. Specific Guidelines

“In addition to legal requirements, special care is taken with data collected from minors, as follows:

- Requiring parental permission for the data collected.
- Making use of awareness tools to encourage minors to obtain permission from parents.”

5. Proactive monitoring

This criterion concerns the internal mechanisms used by the trustmark scheme to monitor the subscriber's compliance with the trustmark program requirements.

5.1. Monitoring mechanisms

This criterion aims to evaluate the concrete procedures of monitoring. Such procedures should be:

- Fair and transparent to the subscribers;
- Based on effective methods (random checks of the merchant's website including mystery shopping, independent verification, reporting requirement for the merchant, frequency, etc.),

5.1.1. Fairness

It is important that the body that conducts the monitoring is independent. As in the Panopticum of J. Bentham, surveillance should be done frequently and on a random basis without the subject being aware of it.

5.1.2. Effectiveness

This criterion refers to the concrete methods for proactive monitoring, notably mystery shopping, regular reporting requirement for Code subscribers (merchants) and modalities of their execution, notably the frequency. The reporting requirement could flag a problem with a Merchant resulting in corrective action.

→ section 7, § 1, ETR

“Trustmark schemes should regularly monitor the subscriber’s compliance with the trustmark requirements. This should include random checks of the subscriber’s site including mystery shopping.”

→ art. 2, § 1, GBDe (C)

“The certifier should put in place effective mechanisms to establish and monitor compliance by the merchant of the trustmark program specifications. These may include random checks by the certifier, independent verification, and/or regular reporting requirements by the merchant.”

→ art. 7, e-Conf. General Principles

“(…). Code owners should take the necessary steps to ensure that they can rapidly detect non-compliance by code-subscribers and take necessary immediate steps to limit damages. (…).”

→ art. 6, § 1, e-Conf. Specific Guidelines

“Code owners are able to properly monitor the effectiveness of the code pro-actively and reactively, either through reporting requirements on code-subscribers on complaints and the outcome of disputes submitted to out-of-court settlement bodies, mystery shopping, audits or other methods. (…).”

→ section 8, al. 2, ETR

“Trustmark schemes should ensure that, when the trustmark requirements are not met, subscribers undertake to amend practices to bring them into line with the trustmark requirements within a short period of time.”

→ art. 6, § 2, e-Conf. Specific Guidelines

“Code subscribers undertake to amend practices to bring them into line with the code at the request of the code owner within a period specified by the code owner (...).”

5.2. Monitoring reports

The object of this criterion is to analyse whether the trustmark scheme reports on the results of the monitoring and the compliance of subscribers.

→ 16, § 1, d) Directive 2000/31/EC on electronic commerce (EC-D)

***“1. Member States and the Commission shall encourage: (...)
(d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce; (...).”***

→ section 7, § 2, ETR

“Trustmark schemes should report on the results of the monitoring and of the non-compliance complaints received to the independent third party.”

→ art. 6, § 1, e-Conf. Specific Guidelines

“(...) Code owners publicise the code to subscribers, consumer representatives and consumers and report on compliance with the code publicly.(...)”

6. Complaint procedure

With this criterion we mean the complaint of a third party, e.g., consumer, member or other person, lodged with the TMS regarding the non-complaint conduct of a member Merchant.

→ art. 10 (Codes of conduct) Proposal for a Directive concerning unfair business-to-consumer commercial practices in the Internal Market (UCP-Prop D)

“This Directive does not exclude the control which Member States may encourage, of unfair commercial practices by code owners of national or Community level codes and recourse to such bodies by the persons or organisations referred to in Article 11 if proceedings before such bodies are in addition to the court or administrative proceedings referred to in that Article.”⁴⁸

→ section 5, ETR

“Trustmark schemes must have the resources necessary to assess applicants, to operate a trustmark scheme and to deal with complaints regarding non-compliance with the trustmark requirements.”

6.1. Accessibility and convenience

This criterion aims to evaluate the “user friendliness” of the complaint procedure. In this respect, the trustmark scheme should ensure:

- Accessibility of the procedure; it must be readily available to consumers or other parties;
- The convenience of the procedure, e.g., use of complaint forms.

In other words, how easy is it to lodge a complaint with the trustmark scheme? Is there a specific entry or application form? Is it an online procedure and how am I informed about the content of the complaint?

→ art. 6, § 1, GBDe (C)

“Access to the certifier must be readily available to consumers and others to accept complaints and to act on them.”

6.2. Quality of the complaint procedure

This criterion aims to concretely evaluate the complaint procedure used by the trustmark scheme. This procedure should be:

⁴⁸ See also art. 11, § 1, al. 3. (enforcement) : “It shall be for each Member State to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints, including those referred to in Article 10”.

- fair and transparent to the parties;
- based on effective methods, notably handling in a short period of time.

6.2.1 Fairness

This criterion mainly relates to the independence of the body that deals with the complaint procedure and the objective of the procedure.

6.2.2 Effectiveness

This criterion relates to the time it takes to handle a complaint in an efficient, transparent and (cost) effective manner.

6.3. Alternative dispute resolution

This criterion concerns the link between the trustmark scheme and alternative dispute-resolution bodies.

It should be noted that with Alternative Dispute Resolution (ADR) we mean that a complaint is not solved by the TMS but is dealt with by an independent Third Party.

→ art. 17 (Out-of-court dispute settlement) Directive 2000/31/EC on electronic commerce (EC-D)

1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.

2. Member States shall 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.

3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce.

→ Commission Recommendation 2001/310/EC on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes (ADR-Rec1)

See pt. B (Transparency):

“1. The transparency of the procedure should be guaranteed

2. Information about the contact details, functioning and availability of the procedure should be readily available to the parties in simple terms so that they can access and retain it before submitting a dispute. (...).”

→ Commission Recommendation 98/257/EC on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes (ADR-Rec2)

→ Preliminary draft proposal for a directive on certain aspects of mediation in civil and commercial matters

→ art. 6, §§ 3 and 4, GBDe (C)

§ 3. “The certifier should offer or, under certain circumstances, as determined in the contract between the certifier and the merchant, require the merchant to offer an alternative dispute resolution (ADR) procedure. ADR systems may be offered by the certifier, the merchant itself or may be outsourced by the merchant.”

§ 4. “In any case, the certifier should respond to consumers’ complaints either by directing consumers to the appropriate mechanism or by contacting the merchant.”

7. Enforcement system

7.1 Quality of the enforcement process

This section concerns the enforcement mechanisms used by the trustmark schemes to ensure that subscribers comply with the trustmark requirements.

In relation to the quality of the enforcement process, the latter should be:

- Fair and transparent to the parties: this means that the trustmark scheme should seek impartiality and objective enforcement. This may include appointing balanced business and consumer representation to the body in charge of the enforcement;
- Based on effective methods: the trustmark scheme should provide for timely and efficient mechanisms in the case of non-compliance by code subscribers.

Furthermore and in relation to the sanctions and their characteristics, the trustmark scheme should:

- Determine dissuasive and proportionate sanctions, including of course the withdrawal of the seal as the most stringent sanction;
- Provide for publicity concerning the sanctions undertaken such as for instance publication on the website, information to the media, etc.

In addition, other mechanisms could also apply, e.g., the right of recourse or appeal.

→ Recommendation 92/295/EEC on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling) (CP-Rec)

“Hereby recommends:

That the trade associations of suppliers: (...)

3. should ensure that their members comply with the codes; (...).”

→ Proposal for a Directive concerning unfair business-to-consumer commercial practices in the Internal Market (UCP-Prop D)

art. 6, § 2. “A commercial practice shall also be regarded as misleading where, in its factual context, taking account of all its features and circumstances, it thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise, and it involves: (...)

(b) non-compliance by the trader with commitments contained in codes of conduct by which the trader has undertaken to be bound, where:

– the commitment is firm and is capable of being verified, and

– information specifying the traders to whom the code applies and the content of the code are publicly available; (...).”

art. 10 (Codes of conduct). “This Directive does not exclude the control which Member States may encourage, of unfair commercial practices by code owners of national or Community level codes and recourse to such bodies by the persons or organisations referred to in Article 11 if proceedings before such bodies are in addition to the court or administrative proceedings referred to in that Article.”

→ section 8, al. 1, ETR

“Trustmark schemes should have an adequate and meaningful enforcement mechanism and should take the necessary steps to ensure that subscribers comply with the trustmarks requirements.”

7.1.1. Fairness

→ section 8, al. 5, ETR

“The enforcement process should be transparent.”

→ art. 2, § 5, GBDe (C)

“The certifier should take all measures to seek impartiality and objective enforcement. This may include appointing independent persons or balanced business and consumer representation to the respective accreditation and enforcement bodies.”

→ art. 4, al. 2, e-Conf. General Principles

“The code owner must demonstrate independence, impartiality and objectivity in all its decisions, notably to grant or withdraw membership of a code; or appoint an independent body to take these decisions. These decisions must be independently verifiable. The code owner should separate its responsibilities as code-owner from any other activities it performs especially where conflicts of interest may arise.”

7.1.2. Effectiveness

→ art. 7, e-Conf. General Principles

“(…) Codes should provide for timely, effective, proportionate and dissuasive sanctions in the case of non-compliance by code-subscribers.”

→ section 8, al. 3 and 4, ETR

3. “A list of dissuasive and proportionate sanctions should be established, which could include information to the media and financial fines.”

4. “Sanctions available should include the withdrawal of the trustmark when the subscriber fails to take action to comply with the trustmark requirements or seriously or repeatedly fails to comply with them.”

→ art. 2, § 3, GBDe (C)

“The type of actions that the certifier can undertake could include:

- withdrawal of the trustmark;***
- public warning about misuse of the trustmark;***
- referral to governmental authorities;***
- legal action against a merchant in breach of the program’s requirements, but who displays the trustmark.”***

→ art. 7, e-Conf. General Principles

“(...) Codes should provide for timely, effective, proportionate and dissuasive sanctions in the case of non-compliance by code-subscribers.”

→ art. 6, § 2, e-Conf. Specific Guidelines

“(...). The sanctions available to code owners should include the ability to withdraw membership of the code when the subscriber fails to take action to comply with the code or seriously or repeatedly fails to comply with the code (...).”

→ section 8, ETR

“Decisions as regards sanctions should be disclosed to the independent third party.”

→ section 8, al. 7, ETR

“Trustmark schemes should make available to the public decisions to withdraw the trustmark.”

→ art. 6, § 2, e-Conf. Specific Guidelines

“(...). Code owners should make available to the public decisions to withdraw membership of the code.”

8. Relationships with protagonists

8.1. General relationships

This section covers the common aspects of the relationships with the consumer, the business and other interested parties. Regarding its relationships with “the public”, a trustmark scheme should:

- Allow interested parties to require additional information or to give input on the performance of the system or any other related element of the trustmark program (the “contact point” could be more than a general email address as *info@trustmarkscheme.com*, but specific geared to the nature of the questions);
- Publish an annual report on its activities;
- Offer additional services such as a press centre, an “events” entry on its website, e.g., to inform about new subscribers, etc.

8.1.1. Feedback

→ section 7, § 3, ETR

“Trustmark schemes should encourage feedback from consumers and other interested parties.”

→ art. 7, § 1, GBDe (C)

“The certifier should include an on-line mechanism to allow interested parties to give input on the performance of the system or any other related element of the trustmark program. The certifier should undertake continuous monitoring on consumers’ satisfaction with the use of the trustmark program by merchants and should take due notice of the surveys’ results.”

→ art. 6, § 1, e-Conf. Specific Guidelines

“(…) Code owners encourage feedback from consumers, other code-subscribers or consumer representatives, about code-subscribers. (…).”

8.1.2. Report on activities

→ Section 2, al. 2, ETR

“Trustmark schemes should publish an annual report on their activities”

8.1.3. Additional services

Does the trustmark scheme offer/have additional services such as a press centre, organisation of awards or events, information for merchants, a newsletter, etc.

8.2. Relationship with consumers

8.2.1. Validity of certification

This criterion mainly refers to the possibility for consumers to easily access details and information of the trustmark scheme, including the trustmark requirements. This can be done by inserting a link on the displayed trustmark seal and by adopting measures that allow the distinction between real and counterfeit trustmarks. Furthermore, information on the seal can be given, by whom it is given, term of validity, reference towards the trustmark scheme, etc.

→ section 3, al. 1, ETR

“(…). By clicking on the trustmark consumers should be able to access easily details of the trustmark scheme, including the trustmark requirements.”

→, GBDe (C)

art. 3, § 3. “Certifiers should ensure that it is clear to consumers what the trustmark certifies (for example, by using a “pop up” screen that briefly describes the program) and that the code of conduct, principles, or best business practices which are the basis of the granting of the trustmark seal are accessible to the consumer, preferably by clicking on the trustmark seal.”

art. 5, § 1. “The certifier should take appropriate measures to ensure that consumers can easily distinguish between real and counterfeit trustmarks. (…).”

→ art. 6, § 3, al. 1, e-Conf. Specific Guidelines

“Codes should require that their trustmarks or any form of identification of membership of a code incorporate links to the related websites so that consumers can easily verify membership and determine its purpose, scope, and standards.”

8.2.2. Privacy Policy

This criterion deals with the protection of personal data. As a data controller, e.g., with regard to a complaint, the trustmark scheme should:

- make reference to a privacy policy in a clear and intelligible way (hyperlink on homepage to privacy policy) and appoint a person responsible for privacy;
- provide information (minimum) on the identity of the controller, the purpose of the procedure, all other parties involved, notably third party processors, and the right of access and rectification.

Although, this concerns in the first place natural persons, we would like to underline that in some European Member States, also legal persons are data subjects in the meaning of 95/46.

8.3. Relationship with businesses

8.3.1. Promotion

This criterion concerns the information provided to businesses on the benefits of participation in the trustmark program and the reasons why one should become a member.

8.3.2. Security and confidentiality

This criterion concerns the security issues related to the trustmark scheme's website and above all the information provided to subscribers in this area. Those responsible for the website should make reference to the security and confidentiality standards (via the publication of a security policy). This is particularly important regarding the data communicated by the merchant for the subscription to the trustmark scheme. Trustmark schemes should also appoint a person responsible for the security of the website (contact point).

4. Conclusions and final remarks

Each of the criteria, both “*must-have*” and “*nice-to-have*” shall be evaluated according to a two-phased procedure:

- Phase 1: **vertical evaluation** of each trustmark scheme with comments on each criterion;
- Phase 2: **horizontal evaluation** of the trustmark schemes assessed in the first phase. During this phase and as a result of the comments made, a value on a scale of five will be given to each criterion⁴⁹.

The advantages of this two-step approach are the following;

- To have an initial understanding of each criteria, the interaction between the different criteria and evaluated trustmark schemes;
- The joint evaluation of the second phase limits the consequences of a single-person subjective evolution.

Eventually, one must be aware that trustmark schemes can undergo modifications. For this reason and to have a more accurate view, we stress that the concerned trustmark schemes should be evaluated within a limited lapse of time.

Once the evaluation is done, conclusions will be formulated.

Conclusions can be formulated with regard to the trustmark scheme concerned or with regard to one or more criteria. Even though most of the attention shall be focussed on the must-have criteria identified above, we shall not limit ourselves to the quality assessment.

⁴⁹ Whereas five reflects the maximum value.

3 Relevant EU regulatory sources (deliverable WP2)

This annex aims to provide an overview of the most relevant EU instruments in the framework of our legal analysis. It does not claim to be exhaustive and includes binding as well as non-binding EU regulations⁵⁰.

1. Commercial Communications/Advertising and Promotion

- § Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in the Internal Market (Directive on electronic commerce)⁵¹ (**EC-D**).
- § Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts⁵² (**DC-D**).
- § Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC⁵³ (**FS-D**).
- § Directive 97/55/EC⁵⁴ of European Parliament and of the Council of 6 October 1997 amending Directive 84/450/EEC⁵⁵ concerning misleading advertising so as to include comparative advertising (**MA-D**).
- § Council Directive 89/552/EEC⁵⁶ of 3 October 1989 on the co-ordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities as amended by Directive 97/36/EC⁵⁷ of the European Parliament and the Council of 30 June 1997.
- § Directive 92/28/EEC of 31 March 1992 on the advertising of medicinal products for human use⁵⁸.
- § Directive 2003/33/EC of the European Parliament and of the Council of 16 May 2003 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising of tobacco products and related sponsorship⁵⁹.
- § Commission proposal for a Regulation of 2 October 2001 on sales promotions in the Internal Market⁶⁰.
- § European Commission proposal for a Directive of 17 June 2003 concerning unfair business-to-consumer commercial practices in the Internal Market⁶¹ (**UCP-Prop D**).

⁵⁰ We also indicate the abbreviation given to each instrument in the “Regulations Table”

⁵¹ *O.J.*, n° L 178, 17-07-2000, p. 1.

⁵² *O.J.*, n° L 144, 04-06-1997, p. 19.

⁵³ *O.J.*, n° L 271, 09-10-2002, p. 16.

⁵⁴ *O.J.*, n° L 290, 23-10-1997, p. 18.

⁵⁵ *O.J.*, n° L 298, 17-10-1989, p. 23.

⁵⁶ *O.J.*, n° L 298, 17-10-1989, p. 23.

⁵⁷ *O.J.*, n° L 202, 30-07-1997, p. 60.

⁵⁸ *O.J.*, n° L 113, 30-04-1992, p. 13.

⁵⁹ *O.J.*, n° L 152, 20-06-2003, p. 16.

⁶⁰ COM(2001) 546.

⁶¹ COM(2003) 0356

2. Pre-contractual information

- § Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in the Internal Market (Directive on electronic commerce)⁶² (**EC-D**).
- § Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts⁶³ (**DC-D**).
- § Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers⁶⁴ (**IP-D**).
- § Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC⁶⁵ (**FS-D**).
- § European Commission proposal for a Directive of 17 June 2003 concerning unfair business-to-consumer commercial practices in the Internal Market⁶⁶ (**UCP-Prop D**).

3. Conclusion of the contract and contractual obligations

- § Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in the Internal Market (Directive on electronic commerce)⁶⁷ (**EC-D**).
- § Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts⁶⁸ (**DC-D**).
- § Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC⁶⁹ (**FS-D**).
- § Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts⁷⁰ (**UT-D**).
- § Directive 1999/44/EC May 25, 1999 on certain aspects of the sale of consumer goods and associated guarantees⁷¹ (**GG-D**).
- § Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit⁷².
- § Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures⁷³.

⁶² O.J., n° L 178, 17-07-2000, p. 1.

⁶³ O.J., n° L 144, 04-06-1997, p. 19.

⁶⁴ O.J., n° L 171, 07-07-1999, p. 12.

⁶⁵ O.J., n° L 271, 09-10-2002, p. 16.

⁶⁶ COM(2003) 0356

⁶⁷ O.J., n° L 178, 17-07-2000, p. 1.

⁶⁸ O.J., n° L 144, 04-06-1997, p. 19.

⁶⁹ O.J., n° L 271, 09-10-2002, p. 16.

⁷⁰ O.J., n° L 095, 21-04-1993, p. 29.

⁷¹ O.J., n° L 171, 07-07-1999, p. 12.

⁷² O.J., n° L 042, 12-02-1987, p. 48.

⁷³ O.J., n° L 13, 19-01-2000, p. 12.

- § European Commission proposal for a Directive of 17 June 2003 concerning unfair business-to-consumer commercial practices in the Internal Market⁷⁴ (**UCP-Prop D**).

4. Payment

- § Commission Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder⁷⁵ (**EP-Rec**).
- § European Commission Communication of 2 December 2003 concerning a 'New legal framework for payments in the Internal Market'⁷⁶.

5. Complaints and redress

- § Commission Recommendation 2001/310/EC of 4 April 2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes⁷⁷ (**ADR-Rec1**).
- § Commission Recommendation 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes⁷⁸ (**ADR-Rec2**).
- § Preliminary draft proposal for a directive on certain aspects of mediation in civil and commercial matters⁷⁹.

6. Privacy and security

- § Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁸⁰ (**DP-D**).
- § Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the telecommunications sector (Directive on privacy and telecommunications)⁸¹ (**PT-D**).
- § European Commission Communication of 26 January 2001 on 'Creating a safer information society by improving the security of information infrastructures and combating computer related crime'⁸².
- § European Commission proposal for a Council framework decision of 19 April 2002 on attacks against information systems⁸³.

⁷⁴ COM(2003) 0356

⁷⁵ O.J., n° L 208, 02-08-1997, p. 52.

⁷⁶ COM(2003) 718.

⁷⁷ O.J., n° L 109, 19-04-2001, p. 56.

⁷⁸ O.J., n° L 115, 19-04-2001, p. 31.

⁷⁹ http://europa.eu.int/comm/justice_home/ejn/news/news_adr_draft_proposal_en.pdf.

⁸⁰ O.J., n° L 281, 23-11-1995, p. 31.

⁸¹ O.J., n° L 201, 30-07-2002, p. 37.

⁸² COM(2000) 890

⁸³ COM(2002) 173

7. Illegal and harmful content and Protection of minors

- § European Parliament and Council Decision N° 276/1999/EC of 25 January 1999 'adopting a multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks'⁸⁴ (**IHC-De**).
- § European Commission proposal for a Council framework decision of 28 November 2001 on combating racism and xenophobia⁸⁵ (**RX-Prop D**).
- § Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity⁸⁶ (**M-Rec**).
- § Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography⁸⁷.
- § Proposal for a Recommendation of the European Parliament and of the Council on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry⁸⁸.

8. Codes of conduct

- § Commission Recommendation 92/295/EEC of 7 April 1992 on codes of practice for the protection of consumers in respect of contracts negotiated at a distance (distance selling)⁸⁹ (**CP-Rec**).
- § Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in the Internal Market (Directive on electronic commerce)⁹⁰ (**EC-D**).
- § Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts⁹¹ (**DC-D**).

⁸⁴ See proposal for a Council Decision of 22 March 2002 amending the decision N° 276/1999/EC.

⁸⁵ COM(2001) 664

⁸⁶ O.J., n° L 270, 07-10-1998, p. 48.

⁸⁷ O.J., n° L 13, 20-01-2004, p. 44.

⁸⁸ COM(2004) 341

⁸⁹ O. J., L 156, 10-06-1992, p. 21.

⁹⁰ O.J., n° L 178, 17-07-2000, p. 1.

⁹¹ O.J., n° L 144, 04-06-1997, p. 19.

4 Business models analysis (deliverable WP3)

Trustmark scheme	Organisation model	Organisation profile
Confianza Online (E)	Stand-alone	<ul style="list-style-type: none"> § Joint initiative of the Spanish advertising self-regulatory organisation, Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL) and AECE, (Asociación Española de Comercio Electrónico). § Launching date 1 January 2003, still operational. § Scheme is aimed at organisations from any sector. § Trustmark scheme is a service added to an existing larger packet of services. § Other services are information services and online marketing. § Dispute resolution by Confianza Online with escalation to AECE and ultimately Junta Arbitral Nacional de Consumo (third party) is possible. Advertising complaints are directly send to AUTOCONTROL. Both bodies are part of EEJ-Net. § Website owner pays annual fee based on annual turnover.
Euro-label (B)	Hierarchical / network	<ul style="list-style-type: none"> § Pan-European initiative, based on the European Code of Conduct, co-ordinated by EuroCommerce. § Network of national Euro-label certification bodies. § Launching date 1 November 1999, still operational. § Scheme is aimed at organisations from the retail sector. § Trustmark scheme is a service added to an existing larger packet of services. § Other services are lobbying, organisation of events, information services and research activities. § Dispute resolution performed through national alternative dispute-resolution bodies that are part of the European Extra Judicial Network (EEJ-Net). § Website owners pay annual fee (some national certification bodies charge a fee based on size of the company).
Luxembourg e-commerce certified (LU)	Stand-alone	<ul style="list-style-type: none"> § Joint initiative of the Ministère de l'Economie du Luxembourg (founder), professional chambers (Chambres de Commerce et Chambre des Métiers) who together own the trustmark logo and independent accreditation bodies that are accredited by the Office Luxembourgeois d'Accreditation et de Surveillance (OLAS). § Launching date 1 March 2002, but still in the start-up phase. § Scheme is aimed at organisations from any sector. § Trustmark scheme is a service added to an existing larger packet of services. § Other services are organisation of events, information services, research activities and developing certification of candidates. § Dispute resolution performed by Luxembourg e-commerce certified. § Website owner pays fee to accreditation body
Thuiswinkel (NL)	Stand-alone	<ul style="list-style-type: none"> § Initiative of e-retail sector. § Launching date 20 December 2001, still operational. § Scheme is aimed at organisations within the retail sector. § Trustmark scheme is a service added to an existing larger packet of services. § Other services are lobbying, organisation of events, information services, research activities, networking, education and legal services. § Dispute resolution performed by Stichting Geschillencommissie Thuiswinkel or any dispute-resolution body that is a member of the Stichting Geschillencommissies Consumentenzaken or any equivalent dispute-resolution body. For cross-border disputes Thuiswinkel.org sends the complaint to an associated Trustmark scheme. § Website owner pays annual fee based on annual turnover.
Trusted shops (D)	Stand-alone	<ul style="list-style-type: none"> § Private initiative operated by Atradius (70%) and Impact Business & Technology Consulting (30%). § Launching date 1 January 2000, still operational. § Scheme is aimed at organisations from any sector. § Trustmark scheme is the core service to which other services are added. § Other services are lobbying, information services and online marketing. § Dispute resolution performed by Trusted Shops with escalation to alternative dispute resolution. § Website owners pay annual user fee.

Trustmark scheme	Organisation model	Organisation profile
TrustUK (UK)	Hierarchical	<ul style="list-style-type: none"> § Joint initiative of the Alliance for Electronic Business and the Consumers' Association, endorsed by the British government, while the secretariat is provided by DMA § TrustUK accredits trustmark schemes that comply with the TrustUK code of practice. § Launching date 1 January 2000, still operational. § Scheme is aimed at organisations from any sector. § Trustmark scheme is the only service provided. § Other services are information services and online marketing. § Dispute settlement performed by TrustUK in case consumer dispute cannot be settled by an accredited trustmark scheme. § Trustmark scheme pays fixed annual fee to TrustUK.
Web Trader (NL)	Network	<ul style="list-style-type: none"> § Joint initiative of European consumer organisations, each using their (different) national codes of conduct. § Launching date 6 June 2000, seized operation on 1 June 2002. § Scheme was aimed at organisations from any sector. § Trustmark scheme was the only service provided (to businesses). § Dispute resolution performed by national consumer organisation, while consumer organisations assisted each other in case of cross-border disputes. § Trustmark was free of charge.
WebTrust (USA/NL)	Hierarchical	<ul style="list-style-type: none"> § Initiative of American Institute of Certified Public Accountants (AICPA) § CPAs are licensed directly by AICPA to perform WebTrust certification service § National accountancy associations pay a fee to IACPA § Launching date 1 June 1999, still operational. § Scheme is aimed at organisations from any sector. § Trustmark scheme is a service added to an existing larger packet of services. § Other services are lobbying, organisation of events, information services, research activities and reviews. § Dispute settlement not mandatory. § Website owner pays fixed license fee to CPA. § Point of negotiation is the model where national accountancy associations pay a license fee to IACPA, while CPAs pay a fee to their national accountancy association instead of to IACPA.
QWeb (CH/IT)	Hierarchical / Network	<ul style="list-style-type: none"> § Initiative of IQNet (International Certification Network), based on the QWeb Certification Scheme. § Network of national certification bodies. § Launching date 12 June 2000, still operational. § Scheme is aimed at organisations from any sector that conducts B2C or B2B e-commerce. § Trustmark scheme is a service added to an existing larger packet of services. § Other services are management systems certification. § Dispute settlement performed by the European network of Arbitration Chambers. § Website owners pay annual user fee to certification body.
BBB OnLine (USA)	Stand-alone / network	<ul style="list-style-type: none"> § Initiative of Council of Better Business Bureaus. § Service provided by local Better Business Bureaus. § Launching date April 1997, still operational. § Scheme is aimed at organisations from any sector. § Trustmark scheme is a service added to an existing larger packet of services. § Other services are information services, consumer reports on companies and charities, consumer complaint handling, advertising review, consumer education. § Dispute settlement performed by Better Business Bureaus. § Website owners pay annual user fee.

5 Trustmark scheme questionnaire (deliverable WP3)

1. Introduction

ECP.NL and CRID (University of Namur) are commissioned by the European Commission (DG Health and Consumer Protection) to analyse the critical success factors for Trustmark schemes in Europe.

This includes all 25 Member States. ECP.NL functions as project leader of the consortium. The study, that will end by the end of 2004, will include the following aspects:

- § Consumer-confidence analysis (subjective experience of trust);
- § Financial viability of Trustmark schemes;
- § Acceptance of trustmarks by businesses and consumers;
- § Brand-value analysis;
- § Benchmark of Trustmark schemes against the EU guidelines on trustmarks;
- § Legal analysis of Trustmark schemes using the existing EU regulatory framework.

Among other things, we have launched an online questionnaire to obtain insight in business and consumer perspectives. UNICE, BEUC and UEAPME are helping us by requesting their members to fill in the questionnaire.

For the purpose of analysing the financial viability of Trustmark schemes, we would like to conduct a telephone survey with each of the representatives of the Trustmark schemes that are selected for this study. These are: BBB*OnLine*, Confianza Online, Eurolabel, Luxembourg e-commerce certified, Qweb, TrustUK, WebTrader, Webtrust, Thuiswinkel.org and Trusted Shops.

We would like to ask you 15 minutes of your time to participate in the survey.

2. General questions:

2.1 Details:

Organisation's name
 Respondent's name
 Respondent's job title
 Respondent's e-mail address
 Respondent's phone number

2.2 *What is the launching date of your Trustmark scheme?*

.../.../..... [day/month/year]

2.3 *Is the Trustmark scheme still operational?*

- Yes (go to question 2.5)
- no

2.4 *If no, when did the Trustmark scheme cease to be operational?*

.../.../..... [day/month/year]

2.5 *The Trustmark scheme is aimed at organisations*

- within a specific sector
- from any sector

2.6 *The Trustmark scheme is*

- the only service provided
- a service added to an existing larger packet of services
- the core service to which other services are added

2.7 *In case other services are provided, what type of services are these?*

- Lobbying
- Organisation of events
- Information services (e.g., website, brochures, reports, newsletter, etc.)
- Research activities
- Other

2.8 *Did you distinguish a start-up phase (i.e. a period of time spent on preparatory work before trustmarks could actually be issued) and an operational phase?*

- Yes
- No (go to question 4.1)

2.9 *If yes, how long was the start-up phase?*

- 0 - 6 months
- 6 - 12 months
- 12 - 18 months
- 18 - 24 months
- longer than 24 months, namely ... months

3. Start-up phase

§ **Costs**

3.1 *Could you give an estimate of the total costs made during the start-up phase?*

- € 0 - € 50,000
- € 50,000 - € 100,000
- € 100,000 - € 150,000
- € 150,000 - € 200,000
- more than € 200,000 namely €

3.2 *What percentage of the total costs in the start-up phase is directly or indirectly related to the Trustmark activities?*

- £ 0 - 20%
- £ 20 - 40%
- £ 40 - 60%
- £ 60 - 80%
- £ 80 - 100%

3.3 *Which types of costs did you make in the start-up phase for the Trustmark activities?*

- £ Costs to get the initiative started and to create an organisation (e.g., meetings, travel, office, staff, board, legal and communication)
- £ Costs to create a code of conduct or criteria (e.g., legal and technical expertise, meetings, expert groups)
- £ Costs to launch a brand (e.g., marketing and communication costs)
- £ Other

3.4 *What percentage of the total costs were made for*

- Costs to get the initiative started and to create an organisation%
- Costs to create a code of conduct or criteria%
- Costs to launch a brand%
- Other

§ **Revenues**

3.5 *What was your total annual turnover in the start-up phase?*

- £ € 0 - € 50,000
- £ € 50,000 - € 100,000
- £ € 100,000 - € 150,000
- £ € 150,000 - € 200,000
- £ more than € 200,000, namely €

3.6 *What percentage of the total annual turnover in the start-up phase is directly related to the Trustmark activities?*

- £ 0 - 20%
- £ 20 - 40%
- £ 40 - 60%
- £ 60 - 80%
- £ 80 - 100%

3.7 *Which types of revenue did you generate in the start-up phase and what was the source?*

- | | <i>Public source</i> | <i>Private source</i> |
|----------------------------------|----------------------|-----------------------|
| £ Project subsidy | £ | £ |
| £ Permanent subsidy | £ | £ |
| £ Sponsorships (e.g., donations) | £ | £ |
| £ Other | £ | £ |

3.8 *What percentage of the total revenue in the start-up phase was generated through:*

- Project subsidy%
- Permanent subsidy%
- Sponsorships%
- Other%

3.9 *What percentage of the total revenue in the start-up phase was generated through public and private sources?*

- Public source%
- Private source%

§ **Profit or loss**

3.10 *Did you make a profit or a loss in the start-up phase, and how much is this in absolute terms or as a percentage of the annual turnover?*

- £ Yes, €..... (or ...%)
- £ No, €..... (or ...%) (go to question 4.1)

3.11 *In case you made a profit, after how many months did you reach a financial break-even point?*

- £ 0 - 6 months
- £ 6 - 12 months
- £ 12 - 18 months
- £ 18 - 24 months
- £ longer than 24 months, namely ... months

4. Operational phase

§ Costs

4.1 *Could you give an estimate of the average total annual costs after the Trustmark scheme became operational?*

- £ € 0 - € 50,000
- £ € 50,000 - € 100,000
- £ € 100,000 - € 150,000
- £ € 150,000 - € 200,000
- £ more than € 200,000, namely €

4.2 *What percentage of the annual total costs in the operational phase is directly or indirectly related to the Trustmark activities?*

- £ 0 - 20%
- £ 20 - 40%
- £ 40 - 60%
- £ 60 - 80%
- £ 80 - 100%

4.3 *Which types of costs did you make in the operational phase?*

- £ Permanent organisational costs (e.g., staff, office, expertise, travel)
- £ Permanent costs of marketing
- £ Permanent costs to ensure compliance and enforcement (e.g., approval, monitoring, audits, dispute settlement)
- £ Other

4.3 *What percentage of the total annual costs were made for*

Permanent organisational costs%
Permanent costs of marketing%
Permanent costs to ensure compliance and enforcement%
Other%

§ Revenues

4.4 *What was your average annual total turnover after the Trustmark scheme became operational?*

- £ € 0 - € 50,000
- £ € 50,000 - € 100,000
- £ € 100,000 - € 150,000
- £ € 150,000 - € 200,000
- £ more than € 200,000, namely €

4.5 *What percentage of the annual total turnover in the operational phase is directly related to the Trustmark activities?*

- £ 0 - 20%
- £ 20 - 40%
- £ 40 - 60%
- £ 60 - 80%
- £ 80 - 100%

<i>3.7 Which types of revenue did you generate in the start-up phase and what was the source?</i>	<i>Public source</i>	<i>Private source</i>
£ Project subsidy	£	£
£ Permanent subsidy	£	£
£ Sponsorships (e.g., donations)	£	£
£ User fees	£	£
£ "Polluter pays" (rate of handling caused)	£	£
£ Other	£	

4.7 What percentage of the total revenue of the operational phase was generated through:

- Project subsidy%
- Permanent subsidy%
- User fees%
- Sponsorships%
- Polluter pays%
- Other

4.8 What percentage of the total revenue in the operational phase was generated through public and private sources?

- Public source%
- Private source

§ **Profit or loss**

4.8 Did you make a profit or a loss in the operational phase, and how much is this in absolute terms (or as a percentage of the annual turnover)?

- £ Yes, €..... (or ...%)
- £ No, €..... (or ...%) (go to question 5.1)

4.9 In case you made a profit, after how many months from the moment the trustmark scheme became operational did you reach a financial break-even point?

- £ 0 - 6 months
- £ 6 - 12 months
- £ 12 - 18 months
- £ 18 - 24 months
- £ longer than 24 months, namely ... months

5. Critical success factors

5.1 *In case the Trustmark scheme has ended its operations, what was the reason (more than one answer is possible)?*

- Insufficient number of seals were issued
- Lack of stakeholders support for the initiative
- Competition from other Trustmark schemes
- Costs to operate the Trustmark scheme were too high
- Insufficient revenue
- Other

Please explain:

.....
.....
.....
...

5.2 *What critical success factors for setting up and running a Trustmark scheme can you identify?*

.....
.....
.....
...

5.3 *What factors are most crucial?*

.....
.....
.....
...

5.4 *What would you have done differently if you could start all over again?*

.....
.....
.....

6 Consumer questionnaire (deliverable WP4)

Welcome,

The European Commission (DG Health and Consumer Protection) has commissioned ECP.NL and CRID (University of Namur) to analyse the critical success factors for trustmark schemes in Europe. This includes all 25 Member States.

The study includes the following aspects:

- Consumer-confidence analysis (subjective experience of trust)
- Financial viability of trustmark schemes
- Acceptance of trustmarks by businesses and consumers
- Brand-value analysis
- Benchmark of trustmark schemes against the EU guidelines on trustmarks
- Legal analysis of trustmark schemes using the existing EU regulatory framework

The purpose of this online questionnaire is to obtain insight in consumers' perspectives on trustmarks. All members of BEUC have been requested to fill out the questionnaire.

We would like to ask you 10 to 15 minutes of your time to participate in the survey.

Which organisation do you represent?

Where does your organisation reside?

Who does your organisation represent?

1. Consumers
2. Consumer-organisations
3. Other (please specify)

We would like to inform you about the progress of this project. Please enter your e-mail address.

Introduction to the following questionnaire

The questionnaire consists of 14 questions on online trustmarks. Every page with questions has a short introduction.

Most questions require an answer. They are indicated with "**".

Often it is possible to check the N/A box (it means not applicable). Please use this option only if you really cannot answer the question.

The final question will give you the possibility to comment on the subject or the questionnaire.

Thank you!

Page 1 Code of conduct

These questions concern the code of conduct that e-commerce websites have to adopt when they want to join a trustmark scheme.

Please answer the questions thinking of the consumers you represent.

Please choose how important the following properties of a Trustmark scheme are for the acceptance by consumers.

(not important, somewhat important, important, very important, extremely important, N/A)

- The code conforms to the legislation of the consumer's country of residence
- The code conforms to the legislation of the country where the online shop resides
- The code conforms to European Union legislation
- The code states what information the online shop must provide to the consumer so that the consumer can make an informed decision about buying goods

- The code states the necessary steps to conclude a legally binding contract between online shop and consumer
- The Trustmark scheme includes a money-back guarantee in case goods are not delivered to or sent back by the consumer
- The code provides a dispute-resolution procedure (in case of unresolved complaints)
- The code specifies which body is entitled to settle disputes
- The code states how personal data are handled
- The code states what security measures are used
- The code is drafted in co-operation with the government
- The code is drafted in co-operation with a consumer organisation
- The code is drafted in co-operation with a business organisation

Page 2 Enforcement

These questions concern the possibilities to enforce the code of conduct on certified e-commerce websites.

Please answer the questions thinking of the consumers you represent.

Please choose how important the following properties of a trustmark scheme are for the acceptance by consumers.

(not important, somewhat important, important, very important, extremely important, N/A)

- There is a mandatory compliance audit on the financial stability of online shops that want to use the trustmark
- There is a mandatory compliance audit on the legal requirements of online shops that want to use the trustmark (for example contracts terms and conditions of sale privacy statement)
- There is a mandatory compliance audit on the technical security of online shops that want to use the trustmark
- The compliance audit is performed by an auditor who is independent from the trustmark scheme
- The compliance of the certified online shops is monitored at least once a year
- The Trustmark scheme is able to impose sanctions against online shops that don't comply with the code of conduct (for example withdrawal of the trustmark logo)
- The dispute-resolution body is independent from the Trustmark scheme
- The dispute-resolution body is independent from the online shops
- The dispute-resolution body is independent from consumer organisations

Page 3 Organisation

These questions concern the organisation behind a trustmark scheme.

Please answer the questions thinking of the consumers you represent.

Please choose how important the following properties of a trustmark scheme are for the acceptance by consumers.

(not important, somewhat important, important, very important, extremely important, N/A)

- The Trustmark scheme resides in the country where the consumer lives
- The Trustmark scheme resides in the country where the online shop resides
- Consumer organisations are represented in the Trustmark scheme
- Industry organisations are represented in the Trustmark scheme
- The Trustmark scheme is approved by the national government
- The Trustmark scheme is approved by the European Commission

Page 4 Website

These questions concern the website of the trustmark organisation.

Please answer the questions thinking of the consumers you represent.

Please choose how important the following properties of a trustmark scheme are for the acceptance by consumers.

(not important, somewhat important, important, very important, extremely important, N/A)

- The Trustmark scheme includes the possibility to validate the certification of an online shop by clicking the trustmark's logo on the online shops website
- The website of the trustmark shows a list of all certified shops
- The website of the trustmark has an effective and usable navigation
- The website of the trustmark has an online forum where consumers can discuss the certified online shops
- The website of the trustmark offers consumers a system to rate the certified online shops
- The website of the trustmark uses the national language of the consumers you represent

If the website of a Trustmark scheme only uses a foreign language which language would the consumers you represent prefer?

1. English
2. French
3. German
4. Spanish
5. Other (please specify)

If the website of the Trustmark scheme uses only the foreign language you have indicated in the previous question most of the consumers you represent would:

1. Have no confidence in the Trustmark scheme
2. Not be able to understand the information on the website but still have (some) confidence in the Trustmark scheme
3. Be able to understand the information and have (some) confidence in the Trustmark scheme
4. Make no difference between the national language and the aforementioned foreign language

What do the consumers you represent prefer:

1. The website of a Trustmark scheme uses formal language and the information is correct in every detail
2. The website of a Trustmark scheme uses informal language and the information is simplified

Page 5 Brand value

These questions concern the brand value of a Trustmark scheme.

Please answer the questions thinking of the consumers you represent.

Please choose how important the following properties of a Trustmark scheme are for the consumers you represent

(not important, somewhat important, important, very important, extremely important, N/A)

1. The Trustmark scheme is operated by an organisation with a well-known brand
2. The Trustmark scheme has certified online shops with a well-known brand
3. The Trustmark scheme has certified a lot of online shops (more than 100)
4. All the certified online shops combined generate a large market share (more than 75% of the online Business to Consumer market)

Page 6 Logo

These questions concern the trustmark's logo.

Please answer the questions thinking of the consumers you represent.

Which location of a trustmark's logo on the website of a certified shop do you think consumers like best?

1. In the top bar where you usually find the companies logo and banners
2. In the navigation bar on the left which stays visible wherever you are on the site
3. In the navigation bar on the right on the front page only
4. In the centre of the front page where you usually find news and special offers

5. In the bottom bar where you usually find a privacy statement and contact information which remains accessible wherever you are on the site
6. Other (please specify)

Which shape of a trustmark's logo do you think consumers like best?

1. A circle
2. A rectangle
3. An oval
4. A combination of a logo and text
5. Just text
6. Other (please specify)

What sort of design of a trustmark's logo do you think consumers like best?

1. Conservative
2. Modern
3. Relating to the Internet
4. Relating to shopping
5. Relating to a country or the EU (flag)
6. Other (please specify)

Page 7 Results

This page concerns the possible results of Trustmark schemes.

Please state whether you (dis)agree with the following statements about the possible results of trustmarks (disagree completely, disagree a little, agree a little, agree completely, N/A)

- A trustmark causes consumers (who are familiar with the trustmark) to spend more money buying online
- A trustmark causes consumers (who are familiar with the trustmark) to buy online more frequently
- A trustmark causes consumers (who are familiar with the trustmark) to buy from a larger variety of online shops
- A trustmark causes consumers (who are familiar with the trustmark) to give personal details necessary for a transaction to certified online shops more easily
- A trustmark adds brand value to online shops with well-established brands
- A trustmark adds brand value to online shops with less-established brands

Page 8 Additional comments

If you have any comments or questions regarding this survey or our project in general, please leave a message here

7 Business questionnaire (deliverable WP5)

Welcome,

The European Commission (DG Health and Consumer Protection) has commissioned ECP.NL and CRID (University of Namur) to analyse the critical success factors for trustmark schemes in Europe. This includes all 25 Member States.

The study includes the following aspects:

- Consumer-confidence analysis (subjective experience of trust)
- Financial viability of Trustmark schemes
- Acceptance of trustmarks by businesses and consumers
- Brand-value analysis
- Benchmark of Trustmark schemes against the EU guidelines on trustmarks
- Legal analysis of Trustmark schemes using the existing EU regulatory framework

The purpose of this online questionnaire is to obtain insight in business perspectives on trustmarks. All members of UNICE and UEAPME have been requested to fill out the questionnaire.

We would like to ask you 10 to 15 minutes of your time to participate in the survey.

Which organisation do you represent?

Where does your organisation reside?

Who does your organisation represent?

1. Large businesses
2. SME's
3. Large business organisations
4. SME organisations
5. Other (please specify)

We would like to inform you about the progress of this project. Please enter your e-mail address.

Introduction to the following questionnaire

The questionnaire consists of 14 questions on online trustmarks. Every page with questions has a short introduction.

Most questions require an answer. They are indicated with "***".

Often it is possible to check the N/A box (it means not applicable). Please use this option only if you really cannot answer the question.

The final question will give you the possibility to comment on the subject or the questionnaire.

Thank you!

Page 1 Code of conduct

These questions concern the code of conduct that e-commerce websites have to adopt when they want to join a Trustmark scheme.

Please answer the questions thinking of the companies you represent.

Please choose how important the following properties of a Trustmark scheme are for the companies you represent

(not important, somewhat important, important, very important, extremely important, N/A)

- The code conforms to the legislation of the consumer's country of residence
- The code conforms to the legislation of the country where the online shop resides
- The code conforms to European Union legislation

- The code states what information the online shop must provide to the consumer so that the consumer can make an informed decision about buying goods
- The code states the necessary steps to conclude a legally-binding contract between online shop and consumer
- The Trustmark scheme includes a money-back guarantee in case goods are not delivered to or sent back by the consumer
- The code provides a dispute-resolution procedure (in case of unresolved complaints)
- The code specifies which body is entitled to settle disputes
- The code states how personal data are handled
- The code states what security measures are used
- The code is drafted in co-operation with the government
- The code is drafted in co-operation with a consumer organisation
- The code is drafted in co-operation with a business organisation

Page 2 Enforcement

These questions concern the possibilities to enforce the code of conduct on certified online shops.

Please answer the questions thinking of the companies you represent.

Please choose how important the following properties of a trustmark scheme are for the acceptance by companies.

(not important, somewhat important, important, very important, extremely important, N/A)

- There is a mandatory compliance audit on the financial stability of online shops that want to use the trustmark
- There is a mandatory compliance audit on the legal requirements of online shops that want to use the trustmark (for example contracts terms and conditions of sale privacy statement)
- There is a mandatory compliance audit on the technical security of online shops that want to use the trustmark
- The compliance audit is performed by an auditor that is independent from the trustmark scheme
- The compliance of the certified online shops is monitored at least once a year
- The trustmark scheme is able to apply sanctions against online shops that don't comply with the code of conduct (for example withdrawal of the trustmark logo)
- The dispute-resolution body is independent from the trustmark scheme
- The dispute-resolution body is independent from the online shops
- The dispute-resolution body is independent from consumer organisations

Page 3 Organisation

These questions concern the organisation behind a Trustmark scheme.

Please answer the questions thinking of the companies you represent.

Please choose how important the following properties of a Trustmark scheme are for the acceptance by companies.

(not important, somewhat important, important, very important, extremely important, N/A)

- The Trustmark scheme resides in the country where the consumer lives
- The Trustmark scheme resides in the country where the online shop that wants to be certified resides
- Consumer organisations are represented in the Trustmark scheme
- Industry organisations are represented in the Trustmark scheme
- The Trustmark scheme is approved by the national government
- The Trustmark scheme is approved by the European Commission
- The Trustmark scheme has defined clear steps for the application procedure

Which system would the companies you represent prefer:

1. The trustmark is free of charge
2. The fee for the trustmark is low (less than 2,000 Euros per year per company)
3. The fee for the trustmark depends on the size of the company that owns the online shop

4. The fee for the trustmark depends on the revenue of the online shop
5. The fee for the trustmark is high (more than 10,000 Euros per year per company)

Page 4 Website

These questions concern the website of the trustmark organisation.

Please answer the questions thinking of the companies you represent.

Please choose how important the following properties of a trustmark scheme are for the acceptance by companies.

(not important, somewhat important, important, very important, extremely important, N/A)

- The Trustmark scheme includes the possibility to validate the certification of an online shop by clicking the trustmark's logo on the online shops website
- The website of the Trustmark scheme shows a list of all certified shops
- The website of the Trustmark scheme has an effective and usable navigation
- The website of the Trustmark scheme has an online forum where consumers can discuss the certified online shops
- The website of the Trustmark scheme offers consumers a system to rate the certified online shops
- The website of the Trustmark scheme uses the national language of the companies you represent

If the website of a Trustmark scheme only uses a foreign language which language would the companies you represent prefer?

1. English
2. French
3. German
4. Spanish
5. Other (please specify)

If the website of the Trustmark scheme uses only the foreign language you have indicated in the previous question most of the companies you represent would:

1. Have no confidence in the Trustmark scheme
2. Not be able to understand the information on the website but still have (some) confidence in the Trustmark scheme
3. Be able to understand the information and have (some) confidence in the Trustmark scheme
4. Make no difference between the national language and the aforementioned foreign language

What do the companies you represent prefer:

1. The website of a Trustmark scheme uses formal language and the information is correct in every detail
2. The website of a Trustmark scheme uses informal language and the information is simplified

Page 5 Brand value

These questions concern the brand value of a trustmark.

Please answer the questions thinking of the companies you represent.

Please choose how important the following properties of a Trustmark scheme are for the companies you represent

(not important, somewhat important, important, very important, extremely important, N/A)

- The Trustmark scheme is operated by an organisation with a well-known brand
- The Trustmark scheme has certified online shops with a well-known brand
- The Trustmark scheme has certified a lot of online shops (more than 100)
- All the certified online shops combined generate a large market share (more than 75% of the online Business to Consumer market)

Page 6 Logo

These questions concern the trustmark's logo.

Please answer the questions thinking of the companies you represent.

Which location of a trustmark's logo on the website of a certified shop do you think companies like best?

1. In the top bar where you usually find the company's logo and banners
2. In the navigation bar on the left which remains visible wherever you are on the site
3. In the navigation bar on the right on the front page only
4. In the centre of the front page where you usually find news and special offers
5. In the bottom bar where you usually find a privacy statement and contact information which remains visible wherever you are on the site
6. Other (please specify)

Which shape of a trustmark's logo do you think companies like best?

1. A circle
2. A rectangle
3. An oval
4. A combination of a logo and text
5. Just text
6. Other (please specify)

What sort of design of a trustmark's logo do you think companies like best?

1. Conservative
2. Modern
3. Relating to the Internet
4. Relating to shopping
5. Relating to a country or the EU (flag)
6. Other (please specify)

Page 7 Results

This page concerns the possible results of Trustmark schemes.

Please state whether you (dis)agree with the following statements about the possible results of Trustmark schemes

(disagree completely, disagree a little, agree a little, agree completely, N/A)

- A trustmark causes consumers (who are familiar with the trustmark) to spend more money buying online
- A trustmark causes consumers (who are familiar with the trustmark) to buy online more frequently
- A trustmark causes consumers (who are familiar with the trustmark) to buy from a larger variety of online shops
- A trustmark causes consumers (who are familiar with the trustmark) to give personal details necessary for a transaction to certified online shops more easily
- A trustmark adds brand value to online shops with well-established brands
- A trustmark adds brand value to online shops with less-established brands

Page 8 Additional comments

If you have any comments or questions regarding this survey or our project in general, please leave a message here