

UNICE – BEUC  
**e-Confidence** project

## Index

<b>GLOSSARY</b> .....	<b>3</b>
<b>PREAMBLE</b> .....	<b>5</b>
<b>EUROPEAN TRUSTMARK REQUIREMENTS</b> .....	<b>6</b>
1.    HIGH STANDARD, MEASURABILITY AND PURPOSE OF TRUSTMARK SCHEMES .....	6
2.    TRANSPARENCY OF TRUSTMARK SCHEMES FOR CONSUMERS AND BUSINESS .....	6
3.    Accessibility and visibility of trustmark schemes for consumers and business .....	6
4.    Scope and content of trustmark schemes .....	6
<i>Language</i> .....	6
<i>Commercial communications and fair marketing practices</i> .....	7
<i>Children</i> .....	7
<i>Pre-contractual Information</i> .....	7
<i>General</i> .....	7
<i>Information on the goods and services on offer, including price</i> .....	8
<i>Information on the contract (terms and conditions)</i> .....	8
<i>Supplementary to all legally required information and other relevant information the subscriber must provide the following information:</i> .....	8
<i>Confirmation process</i> .....	9
<i>Contractual Performance</i> .....	9
<i>Acknowledgement of order</i> .....	9
<i>Payment</i> .....	9
<i>Security</i> .....	10
<i>Security of system</i> .....	10
<i>Security of payment</i> .....	10
<i>Data protection</i> .....	10
<i>Internal complaints management and dispute settlement for consumer complaints</i> .....	10
5.    Operation of trustmark schemes .....	11
6.    Assessment of applicants for trustmark schemes .....	11
7.    Monitoring system.....	11
8.    Enforcement system .....	11
9.    Technical security .....	11
<b>NEUTRAL THIRD PARTY ASSESSMENT OF TRUSTMARK SCHEMES</b> .....	<b>12</b>
Visual representation of the model.....	12
e-Confidence Committee.....	13
<i>Mission</i> .....	13
<i>Composition</i> .....	13
<i>Functioning</i> .....	13
Independent Third Party .....	15
<i>Definition</i> .....	15
<i>Procedural Requirements</i> .....	16
<i>Approval</i> .....	16
<i>Monitoring</i> .....	16

## GLOSSARY

### 1. e-Confidence initiative:

A European Commission initiative in cooperation with consumer and industry representatives seeking to promote high standards of consumer protection and to encourage the sale of goods and services on the Internet.

### 2. European Trustmark requirements (ETR):

A set of requirements that trustmark schemes wishing to participate in the e-confidence initiative must comply with.

### 3. Trustmark schemes:

Any body providing a trustmark to B2C e-merchants after positive assessment on the basis of own criteria.

### 4. Trustmark requirements:

Set of business practices that a trustmark scheme requires its subscribers to comply with. The trustmark requirements may be presented in the form of a code of practice, a code of conduct, a set of requirements or a list of criteria.

### 5. Trustmark:

A label or visual representation showing participation in a trustmark scheme. A subscriber to a trustmark scheme can display a trustmark if he meets the trustmark requirements.

### 6. Subscriber:

Any B2C e-merchant who uses a trustmark after positive assessment by the trustmark scheme concerned.

### 7. E-merchant:

NO AGREEMENT WAS REACHED
--------------------------

UNICE's definition:

*"Any party offering to sell products and/or services, and/or engaging in advertising and marketing on-line (electronically)."*

BEUC's definition:

*"Any party offering to sell products and/or services on-line".*

### 8. Complaints:

#### a) Consumer complaints:

Complaints of individual consumers to subscribers.

#### b) Compliance complaints:

Complaints about the subscriber's compliance with the requirements of the trustmark scheme that he participates in.

#### c) European compliance complaints:

Complaints about a trustmark scheme's compliance with the European trustmark requirements.

**9. Independent Third Party:**

A third party that the e-Confidence Committee has declared as meeting the definition of an "Independent Third Party" in relation to a specific trustmark scheme.

## *PREAMBLE*

The European trustmark requirements (hereafter ETR) aim to provide a high standard of consumer protection in electronic commerce and encourage the sale of goods and services on the Internet.

The ETR offer a basis for good online practice. They do not seek to override or replace any mandatory provisions at European level. They are supplementary to legal obligations and do not affect consumers' statutory rights.

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 enhance their visibility at European level.

The ETR and the e-confidence initiative should be subject to regular review in order to be able to keep pace with the development of the online market and technological change.

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

## ***EUROPEAN TRUSTMARK REQUIREMENTS***

### **1. HIGH STANDARD, MEASURABILITY AND PURPOSE OF TRUSTMARK SCHEMES**

The aim of trustmark schemes should be to foster consumer trust and confidence in the relationship between businesses and consumers in on-line commercial transactions.

Trustmark schemes must comply fully with relevant EU legislation in relation to any obligation they place on subscribers or any practices they recommend to them, and should require that subscribers take the necessary steps to ensure their compliance with their legal obligations. Trustmark schemes should also comply with the relevant OECD guidelines on electronic commerce.

Trustmark schemes should add value for consumers and subscribers through complementing or supplementing legal obligations. Their performance should be measurable and they should ensure a high level of consumer protection.

Trustmark schemes should promote high levels of customer service which should be responsible, flexible and efficient.

### **2. TRANSPARENCY OF TRUSTMARK SCHEMES FOR CONSUMERS AND BUSINESS**

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.

### **3. Accessibility and visibility of trustmark schemes for consumers and business**

The Trustmark should be easily visible to the consumer. By clicking on the trustmark consumers should be able to access easily details of the trustmark scheme, including the trustmark requirements.

Subscription to a trustmark scheme should, in principle, be open to any interested organisation or person, regardless of their place of establishment. Any decisions to accept or reject applicants as subscribers should not be discriminatory and should be based on transparent membership criteria.

### **4. Scope and content of trustmark schemes**

Trustmark requirements must include the following items:

#### ***Language***

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.

### ***Commercial communications and fair marketing practices***

Subscribers must ensure that all commercial communications are fair and in accordance with good marketing practices as defined, for example, by industry self-regulatory programmes.

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.

### ***Children***

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.

### ***Pre-contractual Information***

#### ***General***

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.

---

\* This does not address whether the laws of any particular jurisdiction apply.

*Information on the goods and services on offer, including price*

Subscribers should provide all relevant information about the goods and services on offer in qualitative and quantitative terms.

Any geographical restrictions on sale must be prominently indicated.

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.

*Information on the contract (terms and conditions)*

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.

*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;
- Regularly updated information about the availability of the good or service and the time for delivery;
- Information on the existence or non-existence of the right of withdrawal and period, if any;
- Information about the return policy including any costs of return;
- Information to consumers that subscribers may reject orders should there be a reasonable suspicion that such orders may be fraudulent;
- Information about the identity of the alternative dispute resolution scheme to which the subscriber adheres (including a link to any relevant website);
- Information about the security and authentication systems the subscriber uses to enable consumers to assess the risk in relying on these systems;
- The subscriber's privacy policy.

### **Confirmation process**

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.

### **Contractual Performance**

#### Acknowledgement of order

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.

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."*

*UNICE's proposal:*

*"The acknowledgement is sent without undue delay, e.g. within 2 working days of receipt of the order."*

Subscribers should provide information on the status of the dispatching process either through e-mail or access to an order-tracking tool.

### **Payment**

NO AGREEMENT WAS REACHED.

*BEUC's proposal:*

*"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:*

*UNICE believes 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)*

## **Security**

### 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.

## **Data protection**

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.

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.

The use of privacy-enhancing technologies is encouraged and information to consumers about them should be provided.

## ***Internal complaints management and dispute settlement for consumer complaints***

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.

When the consumer remains dissatisfied, the subscriber should provide information on the alternative dispute resolution scheme that he adheres to.

Trustmark schemes should have an effective mechanism to deal with complaints of non-compliance with the trustmark requirements.

## **5. Operation of trustmark schemes**

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. Assessment of applicants for trustmark schemes**

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.

## **7. Monitoring system**

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.

Trustmark schemes should report on the results of the monitoring and of the non-compliance complaints received to the independent third party.

Trustmark schemes should encourage feedback from consumers and other interested parties.

## **8. Enforcement system**

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.

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.

A list of dissuasive and proportionate sanctions should be established, which could include information to the media and financial fines.

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.

The enforcement process should be transparent.

Decisions as regards sanctions should be disclosed to the independent third party.

Trustmark schemes should make available to the public decisions to withdraw the trustmark.

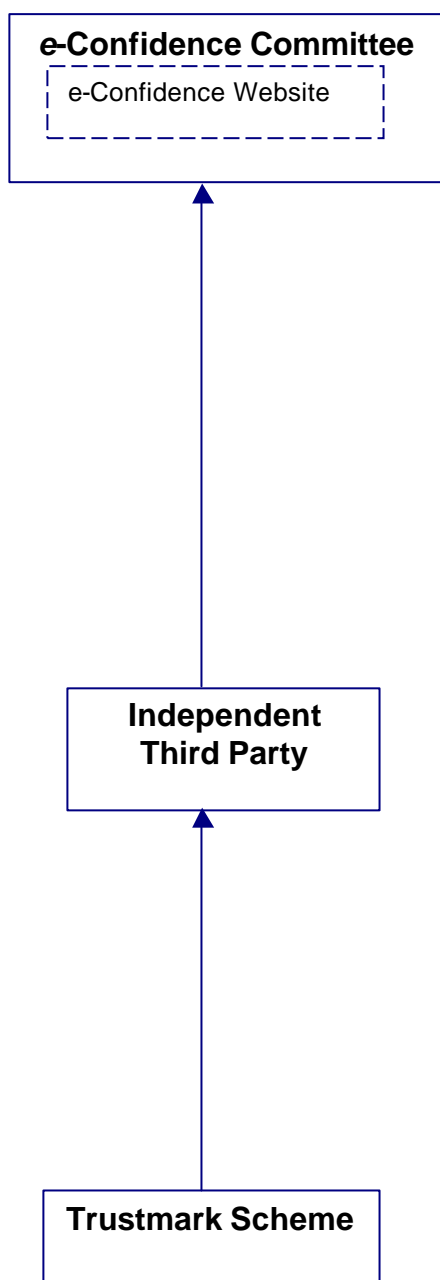
## **9. Technical security**

Trustmark schemes should regularly report on fraudulent use of the trustmark.

Information critical to establishing confidence, and in particular trustmarks, are authenticated using effective technical mechanisms.

## NEUTRAL THIRD PARTY ASSESSMENT OF TRUSTMARK SCHEMES

### Visual representation of the model



The e-Confidence Committee shall

- be responsible for reviewing the whole e-Confidence scheme;
- manage the e-Confidence website;
- have the support of a Secretariat;
- be composed of Equal number of persons proposed and appointed by common accord between UNICE and BEUC. The latter will also appoint by common accord an independent chairman in consultation with the Commission.
- verify that each Third Party that has certified a “*declaration of compliance*” meets the definition of an “Independent Third Party”
- elaborate its internal rules of procedure for dealing with European compliance complaints, including a possible appeal mechanism via arbitration
- elaborate the content of the “*declaration of compliance*” and the “*annual compliance report*” once it is set up;
- send “*declaration of compliance*” forms to Trustmark Schemes and receive the forms duly filled in and certified by an Independent Third Party;
- send “*annual compliance reports*” forms to Trustmark Schemes and receive the forms duly filled in and certified by an Independent Third Party;
- In the case of dispute arising from the interpretation of the European Trustmark Requirements the Committee shall take the final decision;
- Deal with complaints regarding Trustmark Scheme’s compliance with the European Trustmark Requirements (hereafter, European compliance complaints).

**Which Third Party?** Trustmark Schemes will ask an Independent Third Party to certify their “*declaration of compliance*”, To perform this task the latter should meet the definition of an Independent Third Party

#### DEFINITION OF INDEPENDENT THIRD PARTY

An Independent Third Party shall:

- Be independent and seen to be independent so that no facts or circumstances appear, that an informed and reasonable person would question the Recognised Independent Third Party’s ability to act objectively. It must be free from any interest in the results of the assessment;
- Be able to take impartial decisions;
- Have policies and procedures in place that distinguish between the assessment / monitoring task and any other activities the Third Party is engaged in;
- Have the financial resources required for the operation of an assessment / monitoring system for at least one year;
- Have sufficient human resources possessing the necessary abilities, experience, competence and knowledge to perform the assessment task;

#### How does a Trustmark Scheme join the e-Confidence initiative?

1. Request a “*declaration of compliance*” form from the e-Confidence Committee;
2. Fill out the “*declaration of compliance*”;
3. Ask an Independent Third Party to certify the “*declaration of compliance*”;
4. Send the duly completed and certified declaration to the e-Confidence Committee;
5. The latter, when receiving an appropriate application (a duly completed “*declaration of compliance*” form, regularly certified by an Independent Third Party), shall
  - Allow the Trustmark Scheme to add this compliance to its trustmark;
  - Add the Trustmark Scheme to the e-Confidence website.

The Trustmark Scheme shall be informed of its duty to request from the e-Confidence Committee an “*annual compliance report*” form to be completed and certified by an Independent Third Party

## e-Confidence Committee

### **Mission**

The e-Confidence Committee (hereafter 'the Committee') is responsible for:

- reviewing the whole e-Confidence Scheme;
- managing the e-Confidence website;
- verifying for each application that the Third Party which has certified the "*declaration of compliance*" meets the definition of an "Independent Third Party";
- sending "declaration of compliance" forms to Trustmark Schemes and receiving the forms duly completed and certified by an Independent Third Party;
- sending "*annual compliance report*" forms to Trustmark Schemes sufficiently in advance of the expiry date of the initial "*declaration of compliance*";
- taking the final decision regarding the interpretation of the European Trustmark Requirements (hereafter 'the ETR');
- deal with complaints regarding Trustmark Schemes compliance with the ETR;
- elaborating the content of the "declaration of compliance" and the "annual compliance report" once it is set up;
- elaborating its internal rules of procedure for dealing with European compliance complaints, including a possible appeal mechanism via arbitration.

### **Composition**

Equal number of persons proposed and appointed by common accord between UNICE and BEUC. The latter will also appoint by common accord an independent chairman in consultation with the Commission.

### **Functioning**

- The Committee shall have the support of a Secretariat;
- The Secretariat checks that the Third Party meets the definition of a Independent Third Party and reports to the Committee;
- The Committee shall determine whether the Third Party meets the definition of an Independent Third Party by a favourable majority decision.
- The Committee shall promote the e-confidence website and the European Trustmark Requirements;
- In the case of dispute arising from the interpretation of the European Trustmark Requirements the Committee shall take the final decision;
- The Committee when receiving a Trustmark Scheme's certified "declaration of compliance" will verify that an Independent Third Party has performed the certification. It will then proceed to put the Trustmark

Scheme on the e-Confidence website. It will authorise the Trustmark Scheme to insert on its own website a hyperlink to the e-Confidence website<sup>1</sup>;

- In due time before the expiry date of the initial “declaration of compliance”, the Committee will give notice to the Trustmark Scheme of its obligation to submit an “annual compliance report” certified by an Independent Third Party;
- The Committee is responsible for removing non-compliant Trustmark Schemes from the e-Confidence website.

---

<sup>1</sup> We understand that the e-confidence website shall include: the ITP written report on the applicant’s compliance with the European Trustmark Requirements, “Annual compliance reports” certified by Independent Third Parties’ (without information considered by the e-Confidence Committee as confidential), the European Trustmark Requirements, the definition and procedural requirements for Independent Third Parties, a list of approved Trustmark Schemes and information on the e-Confidence Committee.

## Independent Third Party

### *Definition*

The Independent Third Party must be an independent and impartial public or private body, which possesses the abilities, experience, and competence required to carry out its function. The nature of the Independent Third Party (hereafter "ITP") should be such as to ensure that consumers and business can have confidence in its assessment of Trustmark Schemes.

An Independent Third Party shall:

- Be independent and seen to be independent so that no facts or circumstances appear, that an informed and reasonable person would question the ITP's ability to act objectively. It must be free from any interest in the results of the assessment;
- Be able to take impartial decisions;
- Have policies and procedures in place that distinguish between the assessment / monitoring task and any other activities the Third Party is engaged in;
- Have the financial resources required for the operation of an assessment / monitoring system for at least one year;
- Have sufficient human resources possessing the necessary abilities, experience, competence and knowledge to perform the assessment task.

## ***Procedural Requirements***

### *Approval*

The ITP assesses whether a Trustmark Scheme who wishes to appear on the e-confidence website (hereafter “the applicant”) complies with the European Trustmark Requirements. To this effect the ITP will certify the accuracy of the Trustmark Scheme’s “*declaration of compliance*”.

The Independent Third Party shall

- a. proceed to an assessment of the applicant’s compliance with the European Trustmark Requirements by verifying:
  - the accuracy of the applicant’s “*declaration of compliance*”;
  - the applicant’s website (including a verification that an adequate security policy is in place);
  - the compliance of the Trustmarks own requirements with the ETR;
- b. verify that the applicant’s human resources possess the adequate abilities, experience, and competence required to carry out its function;
- c. attach a written report on the applicant’s compliance or non-compliance with the European Trustmark Requirements to the “*declaration of compliance*”. This report includes:
  - clear identification of responsible parties for the assessed Trustmark Scheme;
  - description of the activities of the Trustmark Scheme (e.g.: scope);
  - explanation of compliance;
  - period of validity of the assessment report;
  - signature of authorised member / employee of the Independent Third Party;
- d. inform the applicant of the results of the assessment. When necessary, the Independent Third Party may suggest modifications to the applicant in order for it to comply with the European Trustmark Requirements. Once the necessary modifications have been made, the applicant’s modifications shall be assessed by the Independent Third Party.

### *Monitoring*

An Independent Third Party shall ensure the Trustmark Scheme’s continual compliance with the European Trustmark Requirements by carrying out an annual evaluation through verifying the accuracy of the Trustmark Scheme’s “*annual compliance report*”.

The Trustmark Scheme must, without undue delay, make the appropriate modifications in order for the Independent Third Party to certify its compliance with the European Trustmark Requirements.

The e-Confidence Committee is responsible for removing non-compliant Trustmark Schemes from the e-Confidence website.