## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Adoption of Framework into Codes of Conduct</td>
<td>5</td>
</tr>
<tr>
<td>Practical Implementation</td>
<td>9</td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Access Control Mechanisms</td>
<td>10</td>
</tr>
<tr>
<td>Raising Awareness &amp; Education</td>
<td>14</td>
</tr>
<tr>
<td>Classification of Commercial Content</td>
<td>21</td>
</tr>
<tr>
<td>Fighting Illegal Content on Mobile Community Products or on the Internet</td>
<td>25</td>
</tr>
<tr>
<td>Implementation, Stakeholder Consultation &amp; Review</td>
<td>30</td>
</tr>
<tr>
<td>Appendices</td>
<td>i</td>
</tr>
<tr>
<td>Appendix 1: Reproduction of Original Framework Requirements</td>
<td>ii</td>
</tr>
<tr>
<td>Appendix 2: Framework Signatories</td>
<td>iv</td>
</tr>
<tr>
<td>Appendix 3: Overview of Existing Codes of Conduct by Country</td>
<td>vi</td>
</tr>
<tr>
<td>Appendix 4: Country-by-country Summary of Code Compliance</td>
<td>vii</td>
</tr>
<tr>
<td>Appendix 5: Reproduction of Operator Implementation Questionnaire</td>
<td>x</td>
</tr>
<tr>
<td>Appendix 6: Compliance against Framework Requirements by Country</td>
<td>xxxvii</td>
</tr>
</tbody>
</table>

### DISCLAIMER

PricewaterhouseCoopers LLP ("PwC") have prepared this report relating to Implementation of the European Framework for Safer Mobile Use by Younger Teenagers and Children solely for GSM Association under the terms of GSM Association’s engagement letter with PwC dated 5 January 2009 (the “Engagement”).

PwC accepts no responsibility or liability to any person (except to GSM Association under the relevant terms of the Engagement, including the provisions limiting PwC’s liability) for the preparation and/or content of the report. Accordingly, regardless of the form of action, whether in contract, tort or otherwise, and to the fullest extent permitted by applicable law, PwC neither accepts any liability or responsibility of any kind nor owes any duty of care for the consequences of any person (other than GSM Association on the above basis) acting or refraining to act in reliance on the report or any part thereof or for any decisions made or not made which are based on such report or any part thereof.

This report contains information obtained or derived from a variety of sources as indicated within the report. PwC has not sought to establish the reliability of those sources or verified the information so provided. Accordingly no representation or warranty of any kind (whether express or implied) is given by PwC to any person (except to GSM Association under the relevant terms of the Engagement) as to the accuracy or completeness of the report. Moreover the report is not intended to form the basis of any investment decisions and does not absolve any third party from conducting its own due diligence in order to verify its contents.
The European Framework for Safer Mobile Use by Younger Teenagers and Children (the “Framework”) is a self-regulatory initiative of the European mobile industry, which puts forward recommendations designed to ensure that children can safely access content on their mobile phones by highlighting approaches that had been previously implemented in some EU Member States. As at the 16th April 2009, there are now 81 mobile operators implementing the Framework through the roll-out of national voluntary agreements (“codes of conduct”) and practice.

This report provides an analysis of these national codes of conduct against the requirements of the Framework and also the views of 76 signatory operators across 26 of the Member States regarding the state and basis of their compliance with the Framework.

Adoption of Framework into Codes of Conduct

As noted above, the Framework was designed to provide recommendations on the basis of which operators in each EU Member State could develop a code of conduct specific to their market. In the section of this report entitled Adoption of Framework into Codes of Conduct, we analyse the extent to which these national codes of conduct have been developed and whether they clearly and consistently address all aspects of the Framework.

In its implementation report dated 6 March 2008, the GSM Association concluded that there had been substantial progress towards the development of national codes as “self-regulatory codes of conduct cover 21 EU Member States” and the “industry signatories in these Member States serve around 550 million customers”. Our review confirms this position, with only 2 states not now having in place a dedicated mechanism for the implementation of the Framework. Whilst no national code of conduct exists in 5 countries, 3 of these address this through a commitment from the operators to implement the Framework. Of the remaining two countries, we understand that the signatories to the Framework in Luxembourg have begun discussing a code of conduct. In Belgium, operators are relying on an existing industry code of conduct relating to SMS/MMS/LBS services, which they believe addresses many of the themes of the Framework. Our analysis shows that its scope is narrower such that it does not explicitly address many of the Framework requirements although the code may be supplemented by voluntary initiatives on the part of operators.

Looking at the content of the national codes - a number of which were in place prior to the creation of the Framework - there is a generally high level of consistency between the content of these codes (or other national regulation and/or legislation) and the Framework. In the 21 national codes assessed, the Framework requirements are substantially and explicitly addressed 90% of the time. The areas showing the highest level or alignment are:

• with the exception of Belgium, all national codes explicitly address all Framework requirements in respect of access control mechanisms and classification of commercial content; and

• there is a 100% alignment of all codes with the Framework in relation to requirements 9 and 11, which require the adoption of a classification system capable of distinguishing between “adult” and “other” content, and the need to classify content obtained from third-parties on the same basis.

The key exceptions to this generally high level of alignment are:

• the lack of specific commitments within national codes to build relationships with national authorities for reporting illegal child images (4 of the codes do not specifically address all aspects of requirement 14);

• the lack of specific requirement in the national codes to provide a means for customers to report safety concerns (7 codes do not specifically address all aspects of requirement 6); and

• the lack of commitments to review safety standards once developed (5 codes do not specifically address all aspects of requirement 18).
There is an increased risk that operators will not address these needs as proactively as other areas where they have made explicit commitments. Indeed the responses to the implementation questionnaire did show a higher than average rate of non-compliance in some of these areas although some operators have stated that they are addressing these areas despite the lack of a specific commitment in their country’s code of conduct.

Practical Implementation

In addition to considering the process of development of codes of conduct this report also considers the extent to which mobile operators across the EU have taken action to practically implement the codes and the various approaches taken in different markets.

The detailed responses received from operators show that the majority of operators are content that they are now compliant with most if not all aspects of the Framework.

In particular, there is a high level of stated compliance with respect to Framework recommendations related to access control mechanisms.

- 95% of operators have access control mechanisms in place (82%) or under development (13%) covering both own-branded and third party commercial content.
- Whether through the introduction of classification systems (80%) or policies not to offer adult content (57%), or both, the majority of operators have stated that they are compliant with the aspects of the Framework relating to content classification. However, those operators that rely solely on a policy of not offering adult content are relying on the creator to have classified this content correctly. In this regard, 10% of operators neither contractually oblige suppliers to classify third party commercial content nor do this classification themselves.

There are two areas where the level of implementation is lower, with more than 1 in 5 operators not yet claiming compliance:

- 20% of operators stated that they do not proactively communicate with the relevant local or national law enforcement agencies in their country in order to report any illegal content of which they may become aware, either on their portal or the wider internet. However, in some Member States the appropriate way of dealing with illegal content is to communicate first with a relevant hotline which will then communicate to law enforcement authorities. Some operators are also prevented by local legislation from taking down content unless specifically directed by local law enforcement bodies. In the UK, all operators are members of the Internet Watch Foundation (“IWF”) and block access to websites included on the IWF list. This approach, which is focused solely on illegal child abuse images, may offer a mechanism which avoids some of the potential controversy over censorship by internet service providers. From the responses received, there does not currently appear to be an EU-wide consensus around the scope and mechanisms for blocking illegal content, although this is not a requirement of the Framework. Nevertheless, there is a parallel international initiative – the Mobile Alliance against Child Sexual Abuse Content - which a number of European operators are supporting and which is designed to pro-actively limit access to illegal child images.
- 28% stated that they did not have a separate system in place for customers to report safety concerns. Almost half of these operators are in the 7 Member States where the national code of conduct does not make any explicit commitments to establishing methods for customers to report safety concerns. A number of these operators noted that reports could be handled via their standard customer services. They do not believe that a separate safety helpline for reports from customers to the operator is a productive solution, as it is another number for customers to
remember and may deter reports. However, there is a risk that customers may not be aware that such assistance is available in such cases and operators must ensure that staff are trained to handle reports appropriately.

Finally, whilst 83% of operators already run (67%) or plan to run (16%) awareness campaigns, there are a number of operators that have not yet initiated such plans. The more detailed case studies set out in the report highlight a wide variety of approaches to awareness raising including campaigns focused on point of sale materials, corporate web sites and materials aimed at providing support to teachers, schools and libraries. The content of these campaigns also demonstrates the speed with which issues associated with children's use of mobile phones have evolved and continue to evolve. Many of the materials focus on wider issues such as cyber-bullying, risks associated with the theft of handsets, “happy-slapping” and general (not mobile-specific) internet use.

74% of operators stated that they collaborate with INSAFE, other non-governmental organisations, voluntary associations or other bodies, either to run awareness-raising campaigns or to enable safer internet use for customers. However, the case studies set out in this report which specifically represent such campaigns were highlighted by operators as having been developed either by individual national operators, international operator groups (or groupings of operators and internet service providers) without explicit collaboration with bodies such as INSAFE.
PricewaterhouseCoopers LLP (“PwC”) has been appointed by GSM Association (“GSMA”) to prepare an analysis of the progress made by mobile operators across the 27 EU Member States towards full implementation of the European Framework for Safer Mobile Use by Younger Teenagers and Children (the “Framework”).

The Framework is a self-regulatory initiative of the European mobile industry, which puts forward recommendations designed to ensure that younger teenagers and children can safely access content on their mobile phones. It was finalised in February 2007, following consultation with the European Commission and child protection stakeholders in the context of a High Level Group on Child Protection. A reproduction of the Framework is available in Appendix 1 of this report.

Fifteen signatories at group level (55 national mobile operators) initially signed up to the Framework on Safer Internet Day, 6 February 2007. As at the 16th April 2009, there are now 81 signatory companies implementing the Framework through the roll-out of national voluntary agreements (“codes of conduct”) and practice. These operators are listed in Appendix 2 to this report.

The recommendations of the Framework cover the following areas:

- Classification of commercial content - mobile operators’ own and third-party commercial content should be classified in line with existing national standards of decency and appropriateness so as to identify content unsuitable for viewing by children and younger teenagers;
- Access control mechanisms - appropriate means for parents for controlling children’s access to this content should be provided;
- Education and awareness-raising - mobile operators should work to raise awareness and provide advice to parents on safer use of mobile services, and ensure customers have ready access to mechanisms for reporting safety concern; and
- Fighting illegal content on mobile community products and the internet - mobile operators should work with law enforcement agencies, national authorities and INHOPE or equivalent bodies to combat illegal content on the internet.

The Framework recommendations are not prescriptive, so that operators may implement them in different ways as services, technologies and trends change, as national societal norms vary, and as operators’ services and marketing models differ. This report addresses both the extent to which the Framework has been implemented in the various codes of conduct and legislation in each of the 27 EU countries, and the extent and nature of action taken by signatory operators to implement the requirements of the Framework in practice.

This report is based on a documentary review of each of the codes of conduct detailed in Appendix 3, and on information gathered from operators in the form of a confidential questionnaire as reproduced in Appendix 5. This questionnaire, designed with the assistance of GSMA and sent to each of the 79 signatory operators as at January 2009, was completed in the period from 15 January to 9 March 2009. It provides information on the nature and timing of policies, communications, actions, processes and systems introduced to implement the Framework (further details of the distribution of, and responses to, this questionnaire are provided in the section entitled “Practical Implementation”). We also conducted interviews with selected operators and other stakeholders, as identified in the report, to gather more detailed information on certain specific approaches that operators have adopted to elements of the Framework.

PwC has not sought to establish the reliability of these sources or verified the information provided through the questionnaire or interviews.
Adoption of Framework into Codes of Conduct

Introduction

The European Framework for Safer Mobile Use by Younger Teenagers and Children was issued in February 2007 to put forward recommendations to ensure that younger teenagers and children can access content on mobile phones safely. It was intended that all original and subsequent signatories would implement the Framework though the agreement and implementation of national codes of conduct in each EU Member State.

As of the 16th April 2009, a total of 81 operators in the 27 Member States were signatories to the Framework. These operators are listed in Appendix 2 to this report.

In this section we analyse the stage of development of codes of conduct in each of the Member States, addressing both the existence of a code and also whether each code explicitly covers all aspects of the Framework.

Development of Codes of Conduct

At the time of signature of the Framework in 2007, there were no codes of conduct in place in Austria, Bulgaria, the Czech Republic, Hungary, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia or Spain. As at the 16th April 2009, codes of conduct have since been signed by mobile operators in all of these countries and at present, self-regulatory codes cover 22 EU Member States (see Appendix 3). The industry signatories in these Member States serve around 580 million customers, which represents 96% of all EU mobile subscriptions.

The five countries which have not yet developed such a code have not done so for the following reasons:

- Cyprus, Estonia and Finland have few signatories, and therefore there is not yet an industry consensus on the drafting of a code in these countries. The operators in these countries have committed themselves to comply directly with the requirements of the Framework rather than through a national code. The sole signatory in Cyprus has issued a statement of policy in order to demonstrate its compliance with the requirements of the Framework.
- There was no consensus for industry self-regulation in Luxembourg until recently. We understand that, with the recent signature of the Framework by P&T Luxembourg, the signatories are now considering starting talks either to adapt the existing national Mobile Services Code of Conduct to the Framework or to elaborate a new code of conduct.
- Belgium had an existing industry code of conduct relating to SMS/MMS/LBS services which the industry believes covers many of the requirements of the Framework. This has also been supplemented with voluntary initiatives by the operators. There has therefore been no separate code of conduct developed in this country.

Alignment of Codes of Conduct with the Framework

We have reviewed the codes of conduct (and, where relevant, other formal regulation) of each country to determine the extent to which each code addresses the requirements of the Framework. This analysis is presented below.

Viewed on its own, this analysis does not present a complete view of whether or not operators in each country are compliant with the Framework, but represents only the extent to which the self-regulatory framework developed in each country explicitly aligns with the terms of the Framework, or where some requirements of the Framework are covered by national legislation or formal regulation. Operators can implement (and in some cases our research suggests they have

---

1 Three of the signatories have only signed up to the respective national code of conduct as opposed to signing the Framework.
implemented) further voluntary measures to improve the safety of users or their ability to control access to content. It should also be noted that omissions in the codes may arise because the codes were drawn up before the creation of the Framework, and therefore could not be expected to align exactly with its wording. For example, the original UK code (currently being reviewed and updated) talked only of liaison with law enforcement with respect to fighting illegal content, since the national hotline for reporting illegal content (Internet Watch Foundation) did not exist at the time.
### Alignment of National Codes of Conduct with the Requirements of the Framework

<table>
<thead>
<tr>
<th></th>
<th>Access control mechanisms</th>
<th>Raising awareness &amp; education</th>
<th>Classification of commercial content</th>
<th>Fighting illegal content</th>
<th>Implementation consultation &amp; review</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>N.B.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For descriptions of the Framework requirements, please see full text of Framework provided in Appendix 1.

Austria: Single signatory operator, committed to implement the Framework directly through its own policy statement.

Belgium: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Bulgaria: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Cyprus: Single signatory operator, committed to implement the Framework directly through its own policy statement.

Czech Republic: Small number of signatory operators committed to implement the Framework directly without a national code of conduct.

Denmark: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Estonia: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Finland: Small number of signatory operators committed to implement the Framework directly without a national code of conduct.

France: Single signatory operator, committed to implement the Framework directly through its own policy statement.

Germany: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Greece: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Hungary: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Ireland: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Italy: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Latvia: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Lithuania: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Luxembourg: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Malta: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Netherlands: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Poland: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Portugal: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Romania: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Slovakia: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Slovenia: Code of conduct signed on 31 March 2009. We have therefore not been able to review this code.

Spain: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

Sweden: Single signatory operator, committed to implement the Framework directly without a national code of conduct.

UK: Single signatory operator, committed to implement the Framework directly without a national code of conduct.
The national code (either alone or in combination with other voluntary industry codes, regulation or legislation) is fully compliant with the specific requirements of the Framework;

The national code is compliant in all key aspects. Certain aspects are not explicitly mentioned (as identified in appendix 1 of this report);

There are significant outstanding areas in the national code which means that it does not match the provisions of the Framework.

A more detailed analysis of the codes of conduct by country is provided in Appendix 4.

Overall, the level of correlation between the explicit statements of the national codes and the requirements of the Framework is high. Across the 15 Framework requirements that are relevant to mobile operators, the existing codes (or some other form or regulation / legislation) explicitly align with the Framework approximately 90% of the time, as seen from the number of green areas in the table above. With the exception of Belgium, for example, all national codes address all Framework requirements in respect of access control mechanisms and classification of commercial content. There is also 100% alignment of all codes with the Framework in relation to requirements 9 and 11, concerning the adoption of a classification system capable of distinguishing between “adult” and “other” content, and the need to classify content obtained from third-parties on the same basis.

The areas where the Framework requirements are not addressed as consistently by national codes are predominantly related to specific subsets of requirements. For example, 68% of codes declare an explicit commitment to provide a means for customers to report safety concerns (requirement 6). This is also the case in respect of building relationships with national authorities for reporting illegal child images (requirement 14, 81% alignment) or in order to maintain and review safety standards once developed (requirement 18, 77% alignment). Operators have stated that this is caused at least in part by the fact that these areas rely upon the participation of other stakeholders (e.g. national hotlines) which did not yet exist in some countries at the time the codes were drafted.

There is a risk that operators will not be addressing these recommendations as proactively as other areas where they have made an explicit commitment to certain actions in their codes. The extent of this risk is assessed through the analysis of operators’ compliance in practice, as outlined in the following section of the report.

In the cases where no code of conduct exists to be compared to the Framework, the extent of operators’ compliance can only be assessed through the practical measures implemented. This is also considered in the section below.
Introduction

The recommendations of the Framework were proposed as a means to “provide for safer mobile use by younger teenagers and children across different billing approaches”. As such, the recommendations are not limiting for operators and do not necessarily represent the full extent to which operators have engaged with or implemented practices that achieve this goal. However, they are proposed as a minimum level of activities or behaviours which will enable younger teenagers and children to access content on their mobile devices safely.

The areas into which the Framework is divided are categorised as:

- Access control mechanisms,
- Raising awareness and education,
- Classification of commercial content,
- Fighting illegal content on mobile community products or on the internet, and
- Implementation, stakeholder consultation and review

The original text and recommendations of the Framework are reproduced in Appendix 1.

We considered the specific requirements of each section of the Framework and, through a series of questions posed to each signatory operator, have analysed the industry’s view of the state of practical compliance. The full questionnaire is provided in Appendix 5 to this report. It is important to note that some of the questions addressed activities that go beyond the scope of the Framework. We have also considered the extent of mobile operators' interactions with selected stakeholders and vice versa, as detailed in specific case studies throughout this report.

It should be noted that, although we attempted to obtain data from all 79 of the operators who were signatories of the Framework as at January 2009, we received no response from three of these operators. A further two operators (P&T Luxembourg and Mobitel d.d.) became signatories during the course of our review, and therefore have not been included in the following analysis. The analysis contained in this section therefore does not make reference to the status of implementation of the Framework for these operators (i.e. it contains data from only 76 of the 81 signatories listed in Appendix 2).

A series of charts summarising the responses received according to the relevant area of the Framework is included in Appendix 6 to this report.
Access Control Mechanisms

Summary of Framework requirements

The requirements of the Framework relating to access controls are as follows:

1. Mobile providers should not offer any own-brand commercial content which would be classified as only suitable for adult customers in equivalent media, without providing appropriate means to control access to such content under parental control.

2. Appropriate means to control access to content should also be applied where content is supplied by contracted providers of third party commercial content which would be classified as only suitable for adult customers in equivalent media.

3. Additionally, individual mobile providers should offer capabilities which can be used by parents to customize access to content by children using mobiles. These may include specific services, phones, barring or filtering, and/or billing control.

The extent of practical compliance in each case is summarised below.

Compliance against requirement #1

Operators were asked whether they offered adult content to users of their networks under their own brand, and if so, did they offer means for their users to restrict/block access to this content.

None of the responses indicated that operators offered any own-brand adult content without access control mechanisms in place or under development. 93% of operators are compliant with this requirement at present, as they either provide access controls over any own-branded adult content or do not provide any adult content at all:

- 43 operators stated that they do not offer any adult content under their own brand name. In such a case, operators would not require any additional access controls to be applied in order to comply with the requirement of the Framework.
- 28 out of the 33 operators who do offer adult content under their own brand name have access controls in place over this content.

This makes a total of 71 operators (93%) who comply with the Framework at present. Those operators that have a policy of not offering adult content are reliant on the effectiveness of the design and implementation of their classification systems, as discussed in the appropriate section below.

Only 5 operators (7%) do not currently have access controls over adult content that they offer under their own brand. However, all of these operators stated that they were in the process of developing such mechanisms, with implementation goals varying between February and August of 2009.
Compliance against requirement #2

Operators were asked whether they offered adult content or services created by contracted third party providers to users of their network, and if so, did they offer a means for users to restrict / block access to this content.

The responses indicated that 82% of the operators comply with this requirement. 15 operators (20%) do not offer any third party adult content on their network. These operators are considered compliant by default as they are not required to have controls in place over content they do not offer. Although, as noted in respect of requirement #1 above they are reliant on restrictions in the nature or appropriate classification of content.

Of the 61 operators who do offer third-party adult content, 47 operators do offer access controls over this third-party adult content, and have been deemed compliant. Along with those who offer no adult content this totals 62 operators, or 82%.

Only 1 operator (1%) did not state whether access control mechanisms are applied to contracted third-party adult content, although it appears from descriptions of the mechanisms provided in response to other questions that there is some control over such content by these operators.

A further 10 operators (13%) do not currently have such mechanisms in place but have goals to implement them in the near future, with deadlines ranging from February 2009 to some point in 2010. These are considered semi-compliant in the chart above.

3 operators (4%) stated that they offer third-party adult content that is not restricted by any sort of access control mechanisms, and that they have no plans to implement such mechanisms.

- Two of these operators stated that they rely upon sensible or monitored use of the device to ensure that no inappropriate content is used. The only option provided for access restriction is the complete blocking of all premium content services (an “all or nothing” approach), however there is no sensitivity to the nature of the content that is blocked.

- The third operator indicated that they require proof of identity at the point of purchase of any post-paid contract. Therefore there is a restriction upon underage users being able to obtain a contract that enables them to access inappropriate content. However, this does not relate to pre-paid arrangements, for which no access controls are available.

Since we were unable to establish why these operators do not have more extensive access control mechanisms in place, it appears that they have not fully implemented systems that meet the requirements of the Framework in this area.

Compliance against requirement #3

Operators were asked a variety of questions to establish the nature of any access control mechanisms that they offer and the extent to which these are customisable for the end user, or any services they may design with younger users in mind.

In all, 49 operators (64%) explicitly stated that they offered controls that were customisable in some way, either at purchase or at a later date. The extent of customisability of controls offered by the operators who responded to these
questions varied markedly. Whereas some operators are only in the first stages of implementing mechanisms of any sort, others have developed complex and highly configurable systems to enable the access permissions to be customised according to user needs. A few examples of the diversity of these features have been identified below.

- Operators were asked whether they perform age verification at the point of sale of a mobile device or contract, and what the default access control settings were on their networks or devices.
  - 77% (59 operators) stated that they perform age verification at the point of sale of a mobile device under contract.
  - 3% (2 operators) did not state whether they perform age verification checks or not.
  - 20% (15 operators) do not perform age verification at the point of sale, and 14 of these operators (18%) offer adult content. The ways these operators use age verification as an access control mechanism are shown in the table below:

<table>
<thead>
<tr>
<th>Operators who offer adult content (either own-brand or third-party) but do not perform age verification at point of purchase</th>
<th>14</th>
<th>18%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Of which:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access controls applied as default - age must be verified to change settings</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Access controls applied as default - no data provided about any age verification performed when changed</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Access controls applied as default - no age verification required to change settings</td>
<td>3</td>
<td>4%</td>
</tr>
<tr>
<td>No default controls set - controls can be enabled at a later date</td>
<td>7</td>
<td>9%</td>
</tr>
</tbody>
</table>

These figures show that in practice there is a maximum of 12 operators where there is a risk of children being able to access contracted third-party content without any form of control being applied.

As a further access control mechanism, 23 operators (30%) stated that they perform other checks (such as the salesperson making enquiries of the purchaser) at the point of purchase to identify whether the device is intended for use by a legal minor, and that appropriate controls are therefore applied.

- In some countries there is regulation in force that requires operators or content providers to provide barring for certain content or prohibits marketing to younger users. Countries that have such additional regulation include the Czech Republic, Belgium, Finland, Germany, Italy and the United Kingdom. The requirements of these formal regulations generally coincide with the requirements of the Framework, as they also aim to protect vulnerable users or to allow controls over the distribution of adult content.

- Although it is not an explicit requirement of the Framework, 31 operators (41%) stated that they actively monitor and review the effectiveness of their access control systems. 61 operators in total (80%) either monitor the effectiveness of these systems or provide a means for problems to be reported to them. This leaves only 8 operators (11%) who do neither although, as noted above, this is not a requirement of the Framework.

- 37 operators (49%) stated that they monitor or moderate all chat rooms or similar real-time communications services on their networks. This also goes beyond the requirements of the Framework.

The responses indicate that operators have put in place many different mechanisms to ensure that access to content by younger users is controlled. Moreover, in many cases these measures extend to areas beyond the scope of the Framework, such as making access controls apply by default or moderating chat rooms and forums. The case studies
below provide further examples of the ways in which operators have created access control mechanisms that suit their specific market.

**Telefonica Movistar Spain**

Telefonica Movistar Spain has introduced two mobile phone packages specifically designed for children: the M01 & Playpack. These services offer not only customised interfaces (large keys, bright designs, built-in games, etc) but also specific safety features for younger users.

The M01 (left) is designed for younger users, and provides two main buttons to call parents’ phone numbers directly. Both incoming and outgoing calls are restricted to numbers defined by parents. SMS cannot be sent from the phone, and data stored on the phone can be managed discretely by parents online. The handset also has a built-in phone locator to allow parents to locate their child at any time.

The Playpack offering (right) allows detailed control of numbers that can be called or from which calls can be received, including the ability for the child to call the parents’ numbers even when out of credit, the ability for parents to top up the phone’s credit remotely and the same phone locator service as the M01. In addition, the handset comes pre-loaded with educational games.

It is important to note that Telefonica Movistar’s approach is fairly unusual. The majority of operators do not currently market services directly to children under 16 years of age.

**Mobilkom Austria**

Mobilkom Austria offer two levels of access control settings depending on the type of contract the customer has chosen (post-paid or pre-paid).

For post-paid mobile contracts, content can be restricted based on a user profile which is determined by collecting information at the point of sale. This is generated through identity checks and customer wishes, and will therefore only allow the user to access certain types of content, or use certain services. As Mobilkom Austria requires age verification checks to be performed if the user subsequently wants to change these settings, it is therefore possible to generate a specific service solution for that user that is appropriate to their age and vulnerability.

For pre-paid contracts, the default setting for content controls is unrestricted, and users are only asked to confirm their age if they try to access adult content. However, any adult content which is hosted on Mobilkom Austria’s portal requires a subscription for access; the information obtained at the point of sale of the subscription (which will include the user’s age) can then be used to determine access settings, and to ensure the appropriateness of the content available to the user.

**Vodafone Group**

The Framework calls for access controls to be applied to content which would be classified as adult in equivalent media. In practice, this commitment operates at a national level and requires operators to distinguish between "adult" content and "other" content.

In general, Vodafone's European operating companies support a three category approach where customers are allocated a "child", "teen" or "adult" profile and the content available to a customer reflects national benchmarking or other classification approaches. Typically devices are then set to a default setting when sold and this setting can be changed by the customer or customer's parent provided that he/she meets rules applied by the Vodafone national operator's access control system.

**Conclusion**

The results of our research indicate that the majority of mobile operators have taken action to introduce access control mechanisms in a variety of forms to suit their customers' needs. 100% of operators are - or soon plan to be - compliant in relation to own-brand content, and 95% are or plan to be compliant in relation to third-party content. This area of the Framework is therefore the one that shows the highest overall level of stated compliance across all EU Member States.
Raising Awareness & Education

Summary of Framework requirements

The requirements of the Framework relating to awareness-raising and educational activities are as follows:

4. Mobile providers should provide advice and effective access to information regarding the use of mobile phone services and measures which can be taken by parents to ensure safer use by their children.

5. Mobile providers should encourage customers who are parents to talk to their children about how to deal with issues arising from the use of mobile services.

6. Mobile providers should ensure customers have ready access to mechanisms for reporting safety concerns.

7. Mobile providers should support awareness-raising campaigns designed to improve the knowledge of their customers, through organisations such as the INSAFE network.

8. For these measures to work effectively, policy makers should play a role in improving children’s awareness through updated educational material and approaches. This should include parent and child-friendly information on safer use of mobiles and the internet.

The extent of practical compliance in each case is summarised below.

Compliance against requirement #4

Operators were asked whether they currently run any campaigns, produce educational literature, or have active involvement in any other activities with the aim of increasing awareness about safer mobile use. If this is not the case, operators were asked whether they intend to initiate such activities in the future. In addition, they were asked about the nature of their awareness-raising activities and the different methods used to deliver their messages.

The responses indicated that 83% of operators are currently compliant or have plans in place for future compliance. 63 operators either currently run campaigns (67%) and are therefore currently compliant, or have plans to initiate such activities in the near future (16%) and are shown as semi-compliant in the graph opposite.

Only one operator (1%) did not indicate whether they either currently run, or intend to initiate, any awareness-raising activities in the near future. This leaves 12 operators (16%) who neither run any campaigns at present nor have any intention to do so. These operators do not appear to be complying with the Framework in this area. The geographical distribution of these responses can be seen below.

---

3 INSAFE is a network of national nodes that coordinate Internet safety awareness in Europe.
Although many operators appear to be providing means to encourage safer use by younger teenagers and children (as can be seen in the other sections of this report), the responses indicate that there is scope for more communication with children and parents in a number of territories. There does not seem to be any particular pattern to the geographic spread of compliant and non-compliant operators.

The questionnaire responses indicated a significant variation in the level of and approach to awareness-raising across the EU Member States. Examples of the approaches used include on-screen messages that appear when products are purchased online, articles placed in consumer magazines or continuous engagement with other bodies and organisations promoting similar messages. The case studies below provide some additional examples of campaigns specifically targeted at children via schools and teachers which mobile operators believe have been particularly effective.

These case studies also highlight the fact that the operators’ awareness-raising activities are generally broader than the Framework requirements and do not focus solely on compliance with it. In the cases outlined below, both operators have attempted to address a variety of risks and concerns relating to different new technologies, such as the theft of devices, data protection issues or the use of chat rooms and other internet services. These are not limited to the use of mobile devices or networks, but show a broader attempt to engage with parents who may have concerns about digital convergence as a whole. This reflects an opinion, voiced by some operators, that adopting a single approach or message in reaching this target audience may only have limited success.

The involvement of other stakeholders as requested in requirement #8 of the Framework is therefore also crucial to the effectiveness of such activities. Just as importantly, it can be seen that although many operators are engaged in such activities, and there are many instances of cooperation between operators and other stakeholders such as internet service providers, there is little evidence of cooperation to create combined initiatives on a pan-European level. A notable exception to this is the TeachToday initiative (described below), however most activities are confined to the operators’ local customer bases. This reflects the need to adapt messages to suit national contexts and the commercial need for operators to maintain differentiated offerings in a competitive market.
Orange UK

Orange UK has launched a number of initiatives in the United Kingdom to raise awareness about the safety issues that affect not only customers in general, but also school children, teachers, youth groups and parents. In order to do this, the company has recently developed two DVDs:

- "Incoming Message" - a film about text bullying and what can be done about it, which has been used in 63% of UK secondary schools,
- "Safety Online" - five short movies to provoke debate and discussion around issues such as safe social networking, posting personal information and cyberbullying. This is being used in 54% of UK secondary schools.

Over the last two years, 120 volunteer ambassadors were also recruited from amongst Orange staff and trained to raise awareness on safety issues at schools. They performed 97 school visits around the UK in order to hold discussions about these topics.

In 2008, Orange commissioned Dr Jo Bryce from the University of Central Lancashire to conduct research into how people use the internet. The aim was to establish the extent of the generational digital divide between children and parents to understand where parents needed help. Orange offer a printed guide called "What parents Need to Know", with advice and guidance on phone and internet safety, that is available in all Orange retail stores and, from March 2009, will be included on a CD with every new phone sold.

The company also developed a dedicated website promoting safe and responsible use of products and services (http://www.orange.co.uk/safety), as well as offering professionally moderated Orange teen chat rooms. In 2009, Orange plans to provide a "toolkit" to parents to be delivered at school and parents evenings. This Parent Toolkit will include practical advice, case studies, activities and topics of debate around internet safety issues. Orange also plans to develop resources that are suitable for primary school children in recognition of the fact that children are using the internet and mobile phones at a much younger age than has historically been the case.

Vodafone Czech Republic

Vodafone Czech Republic has adopted the Framework in its approach to offering services to customers, including children and younger teenagers. Central to its response is the recognition that the full range of content previously only available in traditional media (such as newspapers, magazines, TV or video) would become available on the internet and, subsequently, on mobile devices. At the same time, the use of mobile phones by children and young people will continue to increase, bringing this demographic into even closer contact with a huge variety of content.

Vodafone Czech Republic has therefore provided education and practical advice to parents and others in partnership with Čilichili, the most widely-read Czech lifestyle magazine. It also cooperates with the Online Safety Institute (the Czech INSafe node) which is supported by the European Commission’s Safer Internet Programme. To increase awareness of issues arising from this new technology, it supports initiatives in higher education through the University Palacky project, and through the Vodafone Group, it is also active in European Schoolnet and TeachToday.

In the Czech Republic, content which is legal for adults over 18 but illegal or inappropriate for those under this age includes: erotic or violent content, gambling services, chat services, virtual environments and spam content. To protect younger customers, the company has introduced "child" and "adult" user profiles. Where a "child" profile is applied to a mobile device, this consistently restricts access to erotic or other adult content offered on Vodafone’s own mobile portal, through premium voice and SMS services or on web and WAP access, through applying a filter to screen content accessed on the internet. Vodafone was the first Czech company to offer this capability in June 2008.

Finally, with regards to illegal content, Vodafone Czech Republic blocks access to all content identified as illegal child images by the Internet Watch Foundation, the UK-based INHOPE node.
TeachToday.eu

TeachToday is a consortium of mobile operators, social networking providers, content providers and internet service providers. It was set up in 2007 to specifically target teachers in raising awareness about the risks and opportunities associated with children’s use of mobile phones and the internet. An educational website - teachtoday.eu - was launched in Brussels in April 2008 to this end.

The website, available in 6 languages, offers a consistent and comprehensive set of resources for teachers including a guide to technology, essential information on issues such as privacy and personal safety, advice on how to deal with issues as they arise in the classroom and case studies. The different language versions of the website are currently being customised to reflect issues of importance in a number of EU Member States (Czech Republic, France, Germany, Italy, Poland, Spain and the UK) and local launches of the website are planned in the latter half of 2009.

The industry consortium has also worked closely with European Schoolnet, a network of 31 European Ministries of Education, to create the materials and ensure that teachers were consulted throughout the development of the site. The participating companies are Buongiorno, Deutsche Telekom / T-Mobile, Facebook, Google, GSMA, Microsoft, MySpace, Orange France Telecom Group, 02/Telefonica, Telecom Italia and Vodafone.

Compliance against requirement #5

Operators who are actively involved in providing information to users, or who intend to begin doing so in the near future, were asked to describe the main messages that such communications would contain, and the ways in which these messages would be distributed. Although the Framework sets no obligation for operators to provide such information in any particular way, the central message of empowering parents to become involved in promoting safer use by their children is set out in the recommendations. Any further messages may then be adapted to local and national situations.

All the operators who currently undertake such activities, or intend to do so (83% in total - see requirement #4), appear to have integrated this message into their campaigns. All of the operators stated that the explicit messages of their campaigns would contain some, if not all, of the below points:

- The potential dangers of certain multimedia content to the well being (either physical or mental) of younger teenagers or children
- The role of parents / legal guardians / teachers in informing younger teenagers & children of such dangers
- The role of parents / legal guardians / teachers in actively protecting younger teenagers & children from such content through preventing access, monitoring usage, etc.
- The organisations in existence for users to report any concerns about illegal or unsuitable content
- The functionality / controls available to users of mobile services to ensure that younger teenagers & children are using their mobile devices safely and appropriately
- Ways of reacting to and preventing abuse of mobile phones

The means of conveying these messages to parents are varied, but primarily involved reaching customers via email, the operator’s website or through literature available at the point of sale. Some operators also provide hotlines to answer customer concerns, or collaborate with other organisations in order to take these messages directly to the parents and children (such as through school visits).
The diversity of approaches adopted reflects the difficulties to be found in communicating with parents as a homogenous group, as discussed in relation to requirement #4 above. In some countries, such as Austria, the stakeholders involved in drafting the national code of conduct have therefore voluntarily committed themselves to a more cooperative role in promoting such messages. This is achieved through producing further publications and activities (see Vodafone case study above), or through the formation of new bodies with this purpose, such as the Austrian “Kinderkodex”, the FSM in Germany, or participation in initiatives such as TeachToday (see case study above).

It is difficult to gauge the effectiveness of some of these approaches, such as the distribution of literature at the point of sale (we have not performed any verification to confirm whether such literature is actually distributed, made easily available or whether it is actually read by consumers). In addition, in many countries, operators are not necessarily able to collaborate with a local organisation of the nature of INSafe as none exists in their country of operation.

Compliance against requirement #6

Operators were asked whether they have a system in place for customers to report safety concerns related to children’s use of mobile phones, or provide any sort of means for them to do so.

50 operators (66%) stated that they did have a specific system in place for customers to report concerns, quoting email or telephone assistance provided to customers. 5 operators (7%) did not respond to this question, but 21 operators (28%) responded that they did not have a dedicated system. Some operators commented that this was the case because such reports are handled via standard customer care services, and this may be a viable means of compliance if customers are aware of it. However, in such cases there may be a risk that customers are unaware that this reporting option exists. The results presented here therefore only represent those operators who offer a dedicated means of reporting for safety concerns.

In addition, a number of the national codes (32%) fail to make any explicit commitments to establishing methods for customers to report safety concerns. A summary of responses by country is shown below.
Compliance against requirement #7

This requirement is intended to promote cooperation between mobile operators and a variety of other organisations seeking to increase public awareness or safer internet use in different countries. Operators were therefore asked whether they specifically work / plan to work with any organisations to promote awareness of safer mobile use, or whether they support / promote other third-party organisations in other capacities, including hotlines, websites or other international associations for reporting illegal content.

The responses indicated that 74% of operators collaborate in some way with either a reporting entity for illegal content, some sort of non-governmental organisation or family institute, departments of education or even voluntary associations of mobile operators and other stakeholders, such as the FSM in Germany. These collaborations are often entered into alongside any other awareness-raising activities that the operators may undertake. 19 operators (25%) do not have any involvement with other parties in awareness-raising, nor do they support or promote any independent illegal content reporting organisations. This is despite the fact that 18 of these operators indicated that some sort of body or organisation exists in their country which focuses on monitoring and / or preventing illegal content. One operator did not respond.

It should be noted that is not an explicit requirement of the Framework that operators collaborate with reporting entities for illegal content wherever they exist (see the section on “Fighting Illegal Content on Mobile Community Products or on the Internet” below). Nonetheless, the lack of collaboration with these entities is more significant where the operators also show no evidence of collaborating with any other entities to raise awareness. It is not necessarily the case that these operators engage in no awareness-raising activities (see requirements #4-6 above), but simply that they may do so on an entirely individual basis rather than in conjunction with other stakeholders.

Online Safety Institute

The Online Safety Institute is a not-for-profit association, established in 2006 in the Czech Republic. The main objective of the Institute is to promote safer use of the internet and new online technologies, particularly for children, and to fight against illegal content and unsolicited content. In addition, the organisation intends to create a resource of information and professional contacts to act as a repository for best practice and a port-of-call for all child protection stakeholders.

The following approach has been adopted by the Institute:

- Targeting of children / young teenagers (8-12 year-olds) through participatory events and the integration of information on safer internet behaviour in various activities designed for them (such as school visits); and,
- Targeting of adults (parents, teachers, etc) through regional events and workshops, as well as raising questions of safety and awareness in national forums.

The Institute believes that the best way of engaging with children and youngsters is through active and direct means. As examples, they advocate engaging with children via representatives from their own peer group (“ambassadors”) or directly through content created for them, such as educational games or java applets that advocate safer behaviour. This provides a clear platform for mobile operators to participate in providing these opportunities, either through offering such content on their devices or networks or through being involved in the interactions with children and young teenagers. The Institute welcomes participation from operators in the organisation and running of such events, and operators have shown their willingness to be involved on many occasions. In addition, the organisation intends to create a resource of information and content to act as a repository for best practice experiences and a port-of-call for all stakeholders in their individual efforts to increase awareness.

The Institute also believes that the best means of achieving success in increasing awareness is through discussion and collaboration between the relevant stakeholders (including mobile operators) at an educational, non-governmental level rather than through litigation or parliamentary decree. It has recently organised a number of conferences to that effect. The latest Safer Internet Conference took place in December 2008 in Prague and was targeted at mobile operators, internet service providers, content providers, law enforcement bodies and the INSAFE and INHOPE nodes. In this way, the Institute acts not only to create a forum for discussion with mobile operators, but also to involve them in discussions and decision-making processes as responsible stakeholders. It aims to promote a systematic and collaborative approach to identifying the risks presented by online and mobile content and therefore allow operators to work more effectively in addressing them.
The Online Safety Institute is also working to provide operators with a means (which goes beyond the requirements of the Framework) to define “white lists” of acceptable internet content, based on the same technology used to blacklist illegal or inappropriate content in other countries. With this mechanism, users would find pre-approved content advertised by the operator and blocking/self-verification controls implemented for all other content. Their aim is to promote internet sites that offer positive material or content, for example sites that advocate safe and aware internet usage. This could then potentially be used to allow particularly vulnerable users to have access only to “white-listed” content. This approach does not represent any sort of industry consensus on how to provide such controls, however it is an area where the Institute is working with national operators to determine appropriate restrictions and criteria for the system.

Compliance against requirement #8

This requirement is designed to engage stakeholders other than mobile operators in the pursuit of safer mobile and internet use for children and younger teenagers. It is therefore not aimed at mobile operators.

Conclusion

The research shows that awareness raising has been approached in many different ways by operators across the Member States. Several operators have directly initiated or sponsored educational schemes, such as publishing leaflets or providing ambassadors to schools, as seen in the case studies above. However, for many operators collaboration with educational organisations such as TeachToday has been more attractive than initiating such activities independently. Regardless of the exact ways in which they achieve this, 83% of operators are either currently involved in such activities or have plans to be involved soon.

An area of lower compliance is that relating to reporting of safety concerns, where only 66% of operators stated that they have a dedicated means in place for customers to report concerns. Other operators may compensate for this by the presence of customer service lines that can handle such reports, which would constitute compliance in as far as it allows these reports to be made. However there is a risk that customers may not be aware that such assistance is available, and where this is the case, operators must therefore ensure that staff are trained to handle such reports appropriately.
Classification of Commercial Content

Summary of Framework requirements

The requirements of the Framework relating to commercial content classification are as follows:

9 Mobile providers and content providers support classification frameworks for commercial content based on national societal standards and consistent with approaches in equivalent media. Classification of content, whether accessible through telecommunications or not, should be consistent with national societal standards regarding decency, appropriateness and legislation. Classification frameworks should consist of at least two categories: content which is suitable only for adult customers and other content.

10 Mobile providers should ensure that their own-brand commercial content is appropriately classified based on existing national classification standards in the markets where they operate.

11 Through their contractual relationships with professional third party content providers, mobile providers should ensure, after consultation, that these providers classify their commercial content under the same national classification approach.

12 For these measures to work effectively, policy makers, trade associations and other interested parties should support mobile provider initiatives to ensure commercial content providers classify their content against national societal standards.

The extent of practical compliance in each case is summarised below.

Compliance against requirements #9 & #10

Operators were asked whether they use or support a classification framework for their own-brand content that consists of two categories as a minimum: content suitable only for adult customers and other content. They were also asked whether this classification system reflects approaches used in other media in their country of operation. Where operators are using such a system, they can be seen to support it by default. The lack of any such system will also only be relevant where operators are offering content to which it is not applied.

53 operators (69%) have adopted and applied to their own brand content a classification system which reflects the approach used in their country for other media and is capable of distinguishing between “adult” and “other” content. Some of these operators do not actually offer any own-brand adult content.

8 operators, or 11%, stated that they use and apply a content classification system that does not reflect the approach used in other national media. Some of these operators use alternative systems such as WAAT, PEGI or an independent content classification matrix, such as that described in the Vodafone case study below. However, the responses indicate that the effect of any system used is always such that the basic distinction between “adult” and “other” content can be made. Some systems then apply a separate grading to rate the items within these categories (e.g. providing a 1-10 rating for any adult content, or distinguishing between over-16 content and over-18 content).
15 operators (20%) stated that they do not apply any classification to their own-brand content. 8 of these operators (11% of the total) stated that they have adopted a classification system which reflects the approach used in their country for other media, but that they do not apply this to their content as they do not provide any content that would be considered “adult”. Therefore, although these operators have a system capable of distinguishing between “adult” and “other” content in place, they do not apply it to all content and have been considered non-compliant.

This 20% all stated that they do not offer any adult content under their own brand. These operators rely on the classifications applied by the creator of the content to ensure that it is appropriate. They also state that they only offer content of a type (e.g. ringtones, useful information, games) that they believe would not contain any adult material. This group has been considered non-compliant as they provided no further clarification over why their confidence in the supplier’s classification is justified, or whether the suppliers follow the same classification systems. There is therefore a risk that operators who do not have a framework for classification may not detect inappropriate content. However, none of the respondents reported having encountered any problems with misclassification by content providers in the past, which may indicate that their agreements with suppliers are sufficiently rigorous to prevent this being a major issue. This is discussed further below under requirement #11.

Customers can subsequently use safety concern channels (as discussed in the section above) if they have the impression that content may have been wrongly classified. A minority of operators (41%) also actively re-check the classification of content on a regular (weekly or monthly) basis, although this is not a requirement of the Framework.

The table below shows the implementation of these classification systems by country.

The table shows the implementation of these classification systems by country.

<table>
<thead>
<tr>
<th>Country</th>
<th>No. of Operator Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>2</td>
</tr>
<tr>
<td>Belgium</td>
<td>1</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>3</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>4</td>
</tr>
<tr>
<td>Denmark</td>
<td>5</td>
</tr>
<tr>
<td>France</td>
<td>6</td>
</tr>
<tr>
<td>Germany</td>
<td>5</td>
</tr>
<tr>
<td>Greece</td>
<td>4</td>
</tr>
<tr>
<td>Hungary</td>
<td>3</td>
</tr>
<tr>
<td>Ireland</td>
<td>2</td>
</tr>
<tr>
<td>Italy</td>
<td>1</td>
</tr>
<tr>
<td>Latvia</td>
<td>2</td>
</tr>
<tr>
<td>Lithuania</td>
<td>1</td>
</tr>
<tr>
<td>Malta</td>
<td>0</td>
</tr>
<tr>
<td>Netherlands</td>
<td>2</td>
</tr>
<tr>
<td>Poland</td>
<td>4</td>
</tr>
<tr>
<td>Portugal</td>
<td>3</td>
</tr>
<tr>
<td>Romania</td>
<td>1</td>
</tr>
<tr>
<td>Slovakia</td>
<td>0</td>
</tr>
<tr>
<td>Spain</td>
<td>4</td>
</tr>
<tr>
<td>Sweden</td>
<td>3</td>
</tr>
<tr>
<td>UK</td>
<td>2</td>
</tr>
<tr>
<td>Others</td>
<td>6</td>
</tr>
</tbody>
</table>

Question: Do you apply a classification system to your own-brand content that is able to distinguish between “adult” and “other” content, and if so does this reflect the approach used for other media?
Vodafone Group

Vodafone Group has established a content policy which is to be applied internationally but which also integrates the cultural differences in the countries in which it operates. This policy recognises the fact that definitions of acceptable contents vary significantly from one country to another, yet also attempts to ensure that these are addressed consistently across their operations in every country. This policy was designed and implemented prior to the Framework, but allows the group to achieve the same level of control over the nature of content offered to users.

Each country is required to issue a local content proposition, which contains a content review for all content that might be considered inappropriate for younger teenagers or children and the names of the suppliers. The proposition also sets out the various local laws that apply to adult content, along with their requirements, details of their practical implementation and the enforcement of these laws.

The proposition document will then compare the content that the operator provides to a standard “adult erotic matrix” used by the group, which gives a content definition (e.g. lingerie, glamour, etc) depending on the nature of the content. As these definitions, or categories, are indicated by a numerical system ranging from CS1.1 (“lingerie”) to CS10.0 (“Other locally legal sexual activity not detailed above”), the operator can state the numerical level of each content offering. For example, content in one service might be rated as CS1.4, whereas a separate service might be given a rating of CS4.1. This allows distinct content from any supplier or country to be compared to other products according to the criteria of the rating system.

This also allows operators to clearly determine the nature of adult content that they intend to offer. For example, operators in one country may decide that they will not purchase or offer any content that falls within or exceeds a certain rating (e.g. CS3.0 - Genitalia), whereas others may offer content of all ratings. Appropriate controls and warnings can then be implemented in each case.

Each content proposition has to be signed by a national executive sponsor, usually the Chief Marketing Officer, and will be reviewed by Vodafone at group level. This ensures that the management of the local operator is fully involved in, and responsible for, taking measures to ensure content is accurately identified.

Compliance against requirement #11

Operators were asked whether they offer any content provided by a third-party supplier that is adult in nature, and if so, whether this content is then classified by themselves or whether the supplier is contractually obliged to apply a certain classification system.

61 operators (81%) confirmed that they offer third party content that is classified as adult.

- 48 of these operators (64% of the total) state that they have applied their own classification system to this content.
- 6 operators (8% of the total) state that their contracts with suppliers require the content to be pre-classified by the supplier in order to meet the requirements of the Framework (although we have no data in respect of how compliance with these contractual requirements is monitored).
- 7 operators (9% of the total) offer third-party adult content but do not currently either classify this content themselves or require their suppliers to do so. This presents a risk that poor classification systems on the supplier side (or potentially a lack of any classification systems at the supplier) may affect the content provided by the operator. However, most EU jurisdictions require content suppliers to comply with any relevant regulations for the protection of minors, which should help to mitigate this risk.
In 5 of these 7 cases, the operators stated that they are in the process of developing classification systems that they expect to implement between March and August of 2009. The two remaining operators who fall in this category are involved in ongoing discussions in an attempt to define content classifications for the whole market which they do not expect to be resolved until 2010. There is therefore some risk that content may not be correctly classified at present in these cases. Nonetheless, they may be deemed semi-compliant at present.

15 operators (19%) stated that they do not acquire any adult content from third-party suppliers. 11 of these operators (14% of the total) either require this by contract or perform their own content classification to ensure that it is the case, therefore verifying that the content classification is appropriate. One operator, however, stated that it neither includes classification requirements in contracts nor classifies the content received, which presents a risk that it may be affected by poor classification systems on the supplier side and is considered non-compliant. The remaining 3 operators (4%) did not state whether they use either of these methods to verify the nature of content.

Operators were also asked whether third-party providers retained any rights or ability to edit content after its initial classification. Although 11 operators (14%) did not respond, 48 operators (63%) said that suppliers did have the ability to edit content. Only 14 of these (18% of the total) stated that these changes require review or acceptance by themselves. This means that 34 of these operators (45%) may be vulnerable to weaknesses in their content classification that might be caused by undetected content changes made by third parties. However, regulations which apply to suppliers (as mentioned above) should help to reduce this risk. Furthermore, customer channels to voice safety concerns may also provide a way to identify misclassification by suppliers.

**Compliance against requirement #12**

This requirement is designed to engage stakeholders other than mobile network operators in the pursuit of safer mobile and internet use for children and younger teenagers. It is therefore not aimed at mobile operators.

**Conclusion**

80% of operators have adopted and applied a classification system for their own-brand content: 69% have applied a classification system that reflects approaches used in other media and distinguishes between "adult" and "other", while 11% apply some other system to distinguish between “adult” and “other” content. However, 20% of operators rely on the content creator to classify the operators’ own-brand content in line with any system that may be chosen.

With respect to third-party content, 86% of operators have applied a classification system to all content, either performed by the operators themselves or through contractual provisions with their suppliers. This includes 14% of operators who do not provide adult content but perform a classification nonetheless. 9% of operators currently offer third-party adult content but do not either classify this content themselves or contractually require their suppliers to do so. All of these operators have stated that they are currently attempting to resolve this and to become compliant in this area by the end of 2010 at the latest. Only 1 operator (1%) therefore offers adult content but does not either have a compliant classification system in place or intend to introduce one.
Fighting Illegal Content on Mobile Community Products or on the Internet

Summary of Framework requirements

The requirements of the Framework related to combating illegal content on mobile community products or on the Internet are as follows:

13 Mobile providers will continue to work with law enforcement authorities in executing their legislative obligations regarding illegal content.

14 Mobile providers will support national authorities in dealing with illegal child images and, through the INHOPE hotline network or equivalent approaches, will facilitate the notification of this content where hosted on mobile community products or on the Internet.

15 Mobile providers will adopt, or support the creation of, appropriate legally authorized national take-down procedures for such illegal content, including a commitment to liaise with national law enforcement.

16 For these measures to work effectively there should be legal clarity on the nature of content which is illegal and law enforcement authorities (or delegated organizations) should be able to confirm where individual items of content are illegal. This will require the allocation of proportionate law enforcement priority and resources. National governments' support for this is vital.

The extent of practical compliance in each case is summarised below.

Compliance against requirement #13

Operators were asked whether they proactively communicate with local or national law enforcement agencies in their country to report any illegal child abuse content of which they may become aware, either on their portal or the wider internet.

Although two operators (3%) did not respond either way, 53 operators (69%) declared that they do proactively communicate with the relevant law enforcement agencies to report illegal child abuse content of which they may become aware.

The remaining 21 operators (28%) stated that this was not the case. However, in some countries the appropriate way of dealing with illegal content is to communicate first with a relevant hotline such as INHOPE, which will then communicate to law enforcement where required. In these cases operators would not necessarily have a direct relationship with law enforcement except as a last resort, and are therefore not necessarily non-compliant. This is discussed further under requirement #15 below. Based on responses to this question on its own, however, there is potentially scope for these relationships to be improved in order to comply fully with the Framework.

---

4 INHOPE is the International Association of Internet Hotlines.
Compliance against requirement #14

Operators were asked whether they provide a means for customers to report illegal child abuse content to them, or if not, whether they support or promote any hotlines, websites or other means of reporting child abuse content in their country of operation.

Only one operator did not respond either way, whereas 84% (63 operators) declared that they either provide a means for their customers to report illegal child images to them directly (24%), that they support national hotlines or other means of reporting them (17%) or both (43%).

It should be noted, however, that several of those who stated they offer a reporting means for customers do so through their usual customer service channels rather than a specific illegal content reporting route. It is possible that customers may not be aware that the customer service channel can be used for this purpose if it is not advertised, thus diminishing its usefulness. However, some operators commented that they do not necessarily feel a separate reporting line is a productive solution. They feel that it simply provides another number for customers to remember and may deter reports that would otherwise be handled by usual customer service routes.

The remaining 12 (16%) operators indicated that they do not currently offer either of these options. 5 of these (7%) declared that they are either currently in the process of developing links with reporting organisations or their own content reporting facilities. One operator stated that they were not aware of any such organisations within their country of operations with whom they could form such relationships. Therefore only 7 operators (9%) neither offer such reporting routes nor declare any intent to develop them in future, and may be considered non-compliant.

Compliance against requirement #15

Operators were asked whether they have adopted legally authorised national take-down procedures for any illegal content on their servers of which they may become aware, including a commitment to liaise with national law enforcement.

54 operators (71%) stated that they have take-down procedures in place, and 19 operators (25%) said that they do not (the remaining 4% did not answer). However, many of the operators who have not adopted take-down procedures confirmed that they do proactively communicate with relevant international associations (e.g. INHOPE) or national law enforcement to fight illegal content. Some operators might also not offer any own or contractual 3rd party hosting services via their portals.
As discussed in relation to requirement #13, 53 operators (69%) stated that they proactively communicate with local or national law enforcement to report illegal content. When viewed together, these responses indicate that only 13 operators (17%) do not either have take-down procedures in place or work with law enforcement in this area.

It should be noted that in some countries the appropriate way of dealing with illegal content is to communicate first with a relevant hotline such as INHOPE. These organisations will then pass the report to law enforcement if required. In other countries, operators are not allowed to take down any content unless directed to do so by law enforcement. Therefore even where organisations may be available for operators to collaborate with, it may not be possible for them to do so. As a result, non-compliance in this area is likely to be more strongly influenced by national and cultural differences than in certain other areas of the Framework.

Operators were therefore asked whether any such organisations exist in their country of operations, and if so, whether they work with them in order to report illegal content. The responses indicated that alternative reporting organisations exist in all 27 Member States, and 40 operators (53%) stated that they work with such organisations. A total of 60 operators (79%) communicate either with these or with national law enforcement (or both). This is shown in the chart below by country.

Taking this into consideration, only 11% of operators do not have either notice and take-down procedures in place or work with some other organisation to fight illegal child abuse content, and many of these commented that they would remove such content anyway if it was identified by them.

In some cases where reporting organisations exist within the country but operators do not currently collaborate with them, the responses indicated that negotiations to establish such relationships were underway. This may have occurred because the organisations have only recently been established, for example, as in Greece, where operators are sponsoring the development of Saferinternet.gr as a reporting entity but are not yet able to use them as a reporting route.
A specific example of one of the ways in which mobile operators are involved in fighting illegal content is described in the Internet Watch Foundation case study below.

**Compliance against requirement #16**

This requirement is designed to engage stakeholders other than mobile operators in the pursuit of safer mobile and internet use for children and younger teenagers. It is therefore not aimed at mobile operators.

**Internet Watch Foundation**

The Internet Watch Foundation (IWF) is an independent self-regulatory body, funded by the EU and the wider online industry, including internet service providers, mobile operators and manufacturers, content service providers, filtering companies, search providers, trade associations and the financial sector, as well as other organisations for corporate social responsibility reasons. It was established in 1996 to serve as the UK “hotline” for the public and IT professionals to report potentially illegal online content and to be the “notice and take-down” body for such content. The IWF works in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of illegal content, specifically child sexual abuse content hosted anywhere in the world, criminally obscene content and incitement to racial hatred content hosted in the UK.

The foundation works with government to influence initiatives developed to combat online abuse, but this dialogue also goes beyond the UK and Europe to ensure greater awareness of global issues, trends and responsibilities. The foundation works internationally with INHOPE and other relevant authorities and organisations to encourage the wider adoption of good practice in combating online child sexual abuse content and to promote inclusive and united global responses to it. Through involvement with the foundation, therefore, its members (including mobile operators) can participate in this process and generate more effective responses to illegal content, as well as sharing best practices internationally. As an example of this, mobile internet access in the UK only became available after the foundation’s creation, and all mobile operators have therefore been aware of, and made use of, the IWF blacklist since they first introduced mobile internet services, even before the creation of the Framework.

The IWF also helps internet service providers and hosting companies to combat abuse of their networks through a national “notice and take-down” service which alerts them to potentially illegal content on their systems. It also provides data to law enforcement partners worldwide to assist investigations into the distributors of potentially illegal content. As a result of this partnership approach, less than 1% of child sexual abuse content known to the IWF has been hosted in the UK since 2003, down from 18% in 1997. This is clearly a relationship which benefits mobile operators who may be hosting content for users. The foundation also acts as a point of contact and reference for operators or other content providers who may be unsure as to the legality of certain content, helping them to decide how to respond appropriately to it.

As sexually abusive images of children are now primarily hosted abroad, the foundation facilitates an industry-led initiative to protect users from inadvertent exposure to this content by blocking access to it through their provision of a dynamic list of child sexual abuse URLs. The IWF blacklist has been adopted by all UK mobile operators, and is integrated into the access control mechanisms provided by all these operators.

The foundation’s interaction with mobile operators also has a further, reciprocal element in the way that operators are encouraged to promote the foundation’s existence and goals in both their commercial interactions and the awareness of the wider public. The foundation ultimately hopes to encourage all commercial content providers and websites to abide by relevant legal standards, and mobile operators play a significant part in this in the way that they set an example to suppliers through their own involvement with the foundation.

**Conclusion**

The extent to which operators are able to act in response to the requirements linked to fighting illegal content is strongly influenced by differences in national legislation and regulation. Restrictions on banning or blocking of content vary significantly between the EU Member States, as do the relationships between operators and relevant national authorities or other independent organisations. These factors may explain many of the differences in responses discussed above. In summary, 28% of operators do not work actively and directly with law enforcement organisations to respond to illegal content. However, 71% of operators have take-down procedures in place, such that only 13 operators (17%) do not either have their own take-down procedures or work with law enforcement to fight illegal content. Additionally, 84% of operators
stated that they provide some means for customers to report illegal content / support organisations such as the INHOPE hotlines, and 7% of operators have stated that they have plans to do so in the future.
Summary of Framework requirements

The implementation of the Framework through self-regulatory codes at the national level, and the review of any such self-regulatory arrangement, comprise explicit requirements of the Framework. The requirements of the Framework relating to implementation are as follows:

17 Signatory mobile providers and signatory content providers will work towards implementation of this common European Framework through self-regulation at national level in EU Member States. The target for agreement of national self-regulatory codes, consistent with this Framework, is February 2008.

18 Mobile providers will regularly review child safety standards on the basis of the development of society, technology and mobile services in cooperation with European and national stakeholders such as the European Commission, INHOPE and INSAFE.

As shown above, the Framework set a target date for the agreement of national self-regulatory codes of February 2008. However, the implementation of these codes is nationally determined (i.e. the Framework does not set a central implementation deadline for national codes of conduct). Nonetheless, the GSM Association has encouraged all signatories to implement the Framework by August 2009 at the latest.

Compliance against requirement #17

As discussed in the section of this report on Adoption of the Framework into Codes of Conduct, 22 EU Member States have codes of conduct in place as at the 16th April 2009. Only three of these were issued beyond the target date of February 2008 (Malta, Lithuania and Slovenia).

Only three countries have set deadlines for the implementation of these codes that are later than August 2009, as proposed by the GSM Association. The reasons for this are as follows:

- The Czech Republic initially set an implementation goal of December 2010. This was subsequently updated by a collective statement from Czech mobile network operators in which they explained that they were already significantly complying, and that this later deadline was therefore misleading. In this statement, the relevant operators declared that they had already achieved almost total implementation as at January 2009, and that they were making significant and ongoing progress in the areas where implementation was not yet complete.

- Poland set an implementation deadline of February 2009, in line with the suggestions of the Framework. However, the national code allowed a further 6 month leeway for implementation in the event of technical issues preventing the achievement of this target.

- Slovakia set a deadline of December 2009.

From the responses received, the practical compliance of operators in these countries as at April 2009 has been discussed in the preceding section. It does not appear that their later implementation deadlines are significantly delaying the application of the spirit of the Framework.

The results of our survey demonstrate that the majority of operators have responded to most, if not all, aspects of the Framework. Indeed in some cases practical implementation has compensated for gaps in or the lack of national codes of conduct.
Compliance against requirement #18

Operators were asked whether they actively review or refine their policies relating to safer usage of mobile phones by children and younger teenagers on a regular basis, and how this is achieved. They were also asked what sort of bodies or authorities they consult in order to ensure that their policies are kept up-to-date with developments elsewhere.

53 operators (70%) stated that they actively seek to review and refine their policies relating to the use of mobile devices by younger teenagers and children on a regular basis. In many cases, this is also achieved in a passive manner, by an evaluation of any new content partner and the appropriateness of the content received from them for certain age groups. However, certain more active reviews are made possible by the participation of operators in forums relating to safer internet use, for example, which serve to ensure that behaviours and standards across the industry keep track of relevant social developments.

The need for involvement of other stakeholders is clearly indicated in the Framework recommendations that refer to them, either explicitly or as a group (see recommendations 8, 12 and 16). From the discussions that we have held with operators and other stakeholders, as well as the various partners and contacts listed in responses, it appears that operators are engaging with such stakeholders in many ways. Through various arrangements and partnerships, stakeholders are participating in discussions and initiatives that continue to push forward the importance of ensuring a safe environment for younger teenagers and children to use mobile devices and the internet.

Conclusion

The majority of EU Member States have in place some form of code of conduct or other self-regulatory framework that aligns in most respect to the requirements of the Framework. The extent to which these codes of conduct have been implemented in practice is outlined in the previous section.

Whilst 30% of operators stated that they do not have processes in place to actively review their policies relating to mobile phone use by younger teenagers and children on a regular basis, the case studies demonstrate the involvement of many operators with other stakeholders and initiatives. This should help to ensure that the policies adopted remain relevant and that they develop in line with national needs.
Appendices
Appendix 1: Reproduction of Original Framework Requirements

European Framework for Safer Mobile Use by Younger Teenagers and Children

February 2007

European mobile providers and content providers have developed national and corporate initiatives to ensure safer use of mobiles including by younger teenagers and children. These already cover most EU Member States.

Signatory European mobile providers, with support from signatory content providers, now propose an EU-wide common framework to reflect these developments and to encourage all relevant stakeholders to support safer mobile use. This framework will be subject to national implementation by signatory providers.

We recognize:

- mobile services offer an additional way to consume content (still and video images, music, chat, etc.) already offered in other ways - typically by the same providers.
- the importance of parental oversight: accordingly, mobile providers should endeavour to empower parents with information and tools to facilitate their oversight.
- any initiatives to classify content should be based on national societal standards regarding decency, appropriateness and legislation.
- a framework-based approach to industry self-regulation will be effective in adapting to the fast moving environment of mobile technology and services – it will be future proof.

European Mobile Providers – A Responsible Approach

It should be noted that:

Mobile providers only control commercial content they produce themselves or which they commission from professional third parties.

They exert indirect and retrospective control over commercial content in certain other situations, provided there is a contractual relationship with professional third parties.

They are not in a position to control content which is freely accessible on the internet, since there is no relationship between the mobile provider and the content provider.

However, as responsible companies, mobile providers recognise the need to work with customers, parents and other stakeholders, including child protection organizations, in order to promote the safety of younger teenagers and children using mobile services.

Mobile providers offer content which may use pre-pay, post-pay or hybrid approaches to billing. This framework is intended to provide for safer mobile use by younger teenagers and children across different billing approaches.

Recommendations on Safer Mobile Use

Access Control Mechanisms

1. Mobile providers should not offer any own-brand commercial content which would be classified as only suitable for adult customers in equivalent media, without providing appropriate means to control access to such content under parental control.

2. Appropriate means to control access to content should also be applied where content is supplied by contracted providers of third party commercial content which would be classified as only suitable for adult customers in equivalent media.

3. Additionally, individual mobile providers should offer capabilities which can be used by parents to customize access to content by children using mobiles. These may include specific services, phones, barring or filtering, and/or billing control.
Raising Awareness & Education

4 Mobile providers should provide advice and effective access to information regarding the use of mobile phone services and measures which can be taken by parents to ensure safer use by their children.

5 Mobile providers should encourage customers who are parents to talk to their children about how to deal with issues arising from the use of mobile services.

6 Mobile providers should ensure customers have ready access to mechanisms for reporting safety concerns.

7 Mobile providers should support awareness-raising campaigns designed to improve the knowledge of their customers, through organisations such as the INSafe network.

8 For these measures to work effectively policy makers should play a role in improving children's awareness through updated educational material and approaches. This should include parent and child-friendly information on safer use of mobile and the internet.

Classification of Commercial Content

9 Mobile providers and content providers support classification frameworks for commercial content based on national societal standards and consistent with approaches in equivalent media. Classification of content, whether accessible through telecommunications or not, should be consistent with national societal standards regarding decency, appropriateness and legislation. Classification frameworks should consist of at least two categories: content which is suitable only for adult customers and other content.

10 Mobile providers should ensure that their own-brand commercial content is appropriately classified based on existing national classification standards in the markets where they operate.

11 Through their contractual relationships with professional third party content providers, mobile providers should ensure, after consultation, that these providers classify their commercial content under the same national classification approach.

12 For these measures to work effectively policy makers, trade associations and other interested parties should support mobile provider initiatives to ensure commercial content providers classify their content against national societal standards.

Illegal Content on mobile community products or on the Internet

13 Mobile providers will continue to work with law enforcement authorities in executing their legislative obligations regarding illegal content.

14 Mobile providers will support national authorities in dealing with illegal child images and, through the INHOPE hotline network or equivalent approaches, will facilitate the notification of this content where hosted on mobile community products or on the internet.

15 Mobile providers will adopt, or support the creation of, appropriate legally authorized national take-down procedures for such illegal content, including a commitment to liaise with national law enforcement.

16 For these measures to work effectively there should be legal clarity on the nature of content which is illegal and law enforcement authorities (or delegated organizations) should be able to confirm where individual items of content are illegal. This will require the allocation of proportionate law enforcement priority and resources. National governments' support for this is vital.

---

1 INSafe is a network of national nodes that coordinate Internet safety awareness in Europe.

2 INHOPE is the International Association of Internet Hotlines.

Implementation, Stakeholder Consultation & Review

17 Signatory mobile providers and signatory content providers will work towards implementation of this common European framework through self-regulation at national level in EU Member States. The target for agreement of national self-regulatory codes, consistent with this framework, is February 2008.

18 Mobile providers will regularly review child safety standards on the basis of the development of society, technology and mobile services in cooperation with European and national stakeholders such as the European Commission, INHOPE and INSafe.
## Appendix 2: Framework Signatories

<table>
<thead>
<tr>
<th>EU Member State</th>
<th>Mobile Operator</th>
<th>Group Company</th>
<th>Framework Signatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Hutchison 3G Austria</td>
<td>Hutchison Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Mobilkom Austria</td>
<td>Mobilkom Austria Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Orange Austria (One)</td>
<td>Orange France Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>T-Mobile Austria</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Belgium</td>
<td>KPN Base</td>
<td>KPN Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Belgacom Mobile (Proximus)</td>
<td>Belgacom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Mobistar</td>
<td>Mobistar Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Globul</td>
<td>OTE Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>BTC</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Mobiltel Bulgaria</td>
<td>Mobilkom Austria Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Cytamobile</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>MTN</td>
<td>MTN Group</td>
<td>No</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Vodafone Czech Republic</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>T-Mobile Czech Republic</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telefonica O2 Czech Republic</td>
<td>Telefonica Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Denmark</td>
<td>Hutchison 3G Denmark</td>
<td>Hutchison Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Sonofon</td>
<td>Telenor Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>TDC Mobil</td>
<td>TDC Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telia Denmark</td>
<td>TeliaSonera Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>ice.net (Nordisk Mobiltelefon)</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td>Estonia</td>
<td>Tele2 Estonia</td>
<td>Tele2 Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EMT</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Elisa</td>
<td>Elisa Group</td>
<td>No</td>
</tr>
<tr>
<td>Finland</td>
<td>Alands Mobiltelefon</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Sonera</td>
<td>TeliaSonera Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>DNA</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Elisa</td>
<td>Elisa Group</td>
<td>No</td>
</tr>
<tr>
<td>France</td>
<td>Bouygues France</td>
<td>Bouygues</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Orange France</td>
<td>Orange France Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SFR</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>Germany</td>
<td>E-Plus</td>
<td>KPN Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telefonica O2 Germany</td>
<td>Telefonica Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>T-Mobile Deutschland</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Germany</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Greece</td>
<td>Cosmote</td>
<td>OTE Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Wind</td>
<td>Weather Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Greece</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Hungary</td>
<td>T-Mobile Hungary / Magyar Telekom</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Pannon GSM</td>
<td>Telenor Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Hungary</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Ireland</td>
<td>Hutchison 3G Ireland</td>
<td>Hutchison Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telefonica O2 Ireland</td>
<td>Telefonica Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Ireland</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Italy</td>
<td>Meteor</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Hutchison 3G Italy</td>
<td>Hutchison Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>TIM Italy</td>
<td>Telecom Italia Mobile Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Italy</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Latvia</td>
<td>LMT</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Bite Latvia</td>
<td>Bite Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Tele2 Latvia</td>
<td>Tele2 Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Trialtel</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td>EU Member State</td>
<td>Mobile Operator</td>
<td>Group Company</td>
<td>Framework Signatory</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>---------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Omnitel</td>
<td>TeliaSonera Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Bite Lithuania</td>
<td>Bite Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Tele2 Lithuania</td>
<td>Tele2 Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Tango</td>
<td>Belgacom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>P&amp;T Luxembourg</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vox</td>
<td>Mobistar Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Malta</td>
<td>Go Mobile</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Malta</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Netherlands</td>
<td>KPN</td>
<td>KPN Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>T-Mobile Netherlands</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Netherlands</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Poland</td>
<td>P4 (signatory of national code)</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Centertel</td>
<td>Orange France Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>PTC</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Polkomtel</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Portugal</td>
<td>Vodafone Portugal</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>TMN (signatory of nation code)</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Optimus (signatory of national code)</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>Romania</td>
<td>Vodafone Romania</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cosmote Romania</td>
<td>OTE Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Orange Romania</td>
<td>Orange France Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>DigiMobil</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Zapp</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td>Slovakia</td>
<td>Orange Slovakia</td>
<td>Orange France Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telefonica O2 Slovakia</td>
<td>Telefonica Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>T-Mobile Slovensko</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Slovenia</td>
<td>SiMobil</td>
<td>Mobilkom Austria Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Mobitel d.d.</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>T-2</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Tusmobil</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td>Spain</td>
<td>Orange Spain</td>
<td>Orange France Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telefonica Moviles</td>
<td>Telefonica Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone Spain</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Sweden</td>
<td>Yoigo</td>
<td>TeliaSonera Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Hutchison 3G Sweden</td>
<td>Hutchison Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Tele2 Sweden</td>
<td>Tele2 Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telenor Sweden</td>
<td>Telenor Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telia Sweden</td>
<td>TeliaSonera Group</td>
<td>Yes</td>
</tr>
<tr>
<td>UK</td>
<td>ice.net (Nordisk Mobiltelefon)</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Hutchison 3G UK</td>
<td>Hutchison Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Telefonica O2 UK</td>
<td>Telefonica Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>Orange France Telecom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>T-Mobile UK</td>
<td>Deutsche Telekom Group</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Vodafone UK</td>
<td>Vodafone Group</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Appendix 3: Overview of Existing Codes of Conduct by Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Code of Conduct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Voluntary Code of Self-Regulation for Mobile-Telephone Operators- Code of conduct for the safe use of mobile telephones by young people</td>
</tr>
<tr>
<td>Belgium</td>
<td>GOF Guidelines for SMS/MMS/LBS Services</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Code of Conduct on Safer Mobile Use by Children and Younger Teenagers</td>
</tr>
</tbody>
</table>
| **Czech Republic** | [General Rules of Provision of Premium Services (Premium SMS, Premium MMS) 4.1](https://example.com)  
[General Recommendations for the Provision of Audiotex Services 3.2](https://example.com)  
Agreement on Implementation of National Self-Regulation |
| Denmark      | Framework Agreement on Mobile Content and Payment Services                       |
|              | Guidelines for the handling of requests regarding criminal activity on the Internet |
|              | Code of conduct for ISPs in Denmark, covering the enforcement of intellectual property rights |
| France       | Operators’ Code of Conduct Regarding Mobile Multimedia Content                    |
| Germany      | Code of Conduct for Mobile Phone Operators in Germany for the Protection of Minors |
|              | Code of Conduct of the FSM - organisation for the voluntary self-regulation of multimedia service providers |
|              | Protection of Minors in Mobile Communications- Voluntary Commitment by Mobile Communications Providers |
| Greece       | Code of Conduct for Value Added Services Provided through Mobile Phones and for the Protection of Minor Users |
|              | Annex A’ Memorandum for Safer Mobile Use by Children and Younger Teenagers       |
| Hungary      | Hungarian Mobile Telephone Service Providers Self-Regulation Code for Safer Mobile Telephone Use by Young Teenagers and Children |
|              | Appendix no.1 Code of Ethics for Premium Rate Services                           |
| Ireland      | The Irish Mobile Operators Code of Practice for the Responsible and Secure Use of Mobile Services |
| Italy        | Code of Conduct for Premium Services and Child Protection                        |
|              | Code of Practice for premium rate numbers in decade 4 – operative guidelines      |
| Latvia       | Code of Conduct for the Protection of Children in the Field of Mobile Communications in Latvia |
| Lithuania    | Lithuanian National Code of Practice for Safe Use of Mobile Communications by Minors |
| Malta        | Code of Conduct for Electronic Content Provision by Electronic Communications Undertakings in Malta |
| Netherlands  | Code of Conduct for the safer use of mobile telephones for children and young teenagers |
| Poland       | Code of good practice in the area of safe use of mobile phones                   |
| Portugal     | CODE OF CONDUCT FOR ACTIVITIES INVOLVING THE PROVISION OF CONTENT SERVICES        |
| Romania      | Code of Conduct for safely using the content provided on the mobile phone        |
| Slovakia     | National Code for mobile operators on safe use of mobile phones                 |
| Slovenia     | Self-Regulatory Code of Conduct of Mobile Network Operators on the Safer Use of Mobile Devices by Children and Adolescents |
|              | Note: Slovenian operators signed this national code of conduct on 31 March 2009. We were not able to review the code as part of our analysis. |
| Spain        | Code of Conduct for mobile operators designed to encourage responsible use by underage persons of electronic content serviced supplied via mobile telephone networks in Spain |
| Sweden       | Ethical Rules for Premium Rate Call Services                                     |
|              | Code of Conduct - Mobile Premium Services                                        |
|              | Code of conduct- Safer use of mobile phones and services by younger teenagers and children |
| UK           | UK Code of Practice for the Self-regulation of New Forms of Content on Mobiles    |

For further information, visit [http://www.gsmeurope.org/safer_mobile/national.shtml](http://www.gsmeurope.org/safer_mobile/national.shtml)
Appendix 4: Country-by-country Summary of Code Compliance

<table>
<thead>
<tr>
<th>Framework recommendation</th>
<th>Austria</th>
<th>Belgium</th>
<th>Bulgaria</th>
<th>Cyprus</th>
<th>Czech Republic</th>
<th>Denmark</th>
<th>Estonia</th>
<th>Finland</th>
</tr>
</thead>
</table>
| #1 Mobile providers should ensure customers have ready access to information regarding the use of mobile phone services and mechanisms which can be taken by parents to ensure their children.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code does not explicitly address this requirement. |
| #2 Appropriate means to control access to content should also be applied where content is supplied by contracted providers of third party content and content which would be classified as unsuitable for adult customers is explicit in the content.
| Code explicitly addresses this requirement. |
| | Code explicitly addresses this requirement. |
| | Code does not explicitly address this requirement. |
| #3 Appropriate means to control access to content should also be specialist because content is supplied by contracted providers of third party content, and content which would be classified as unsuitable for adult customers is not explicit in the content.
| Code explicitly addresses this requirement. |
| | Code does not explicitly address this requirement. |
| | | Code explicitly addresses this requirement. |
| #4 Mobile providers should provide advice and effective access to customer service responsibilities.
| Code explicitly addresses this requirement. |
| | Code does not explicitly address this requirement. |
| | | Code explicitly addresses this requirement. |
| #5 Mobile providers should encourage customers who are parents to sign up to mobile services.
| Code explicitly addresses this requirement. |
| | Code does not explicitly address this requirement. |
| | | Code explicitly addresses this requirement. |
| #6 Mobile providers should ensure that their own-brand commercial content is similar to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #7 Mobile providers should support awareness-raising campaigns designed to improve the knowledge of their customers, through, for example, the use of special codes.
| Code explicitly addresses this requirement. |
| | Code does not explicitly address this requirement. |
| | | Code explicitly addresses this requirement. |
| #8 Mobile providers should ensure appropriate mechanisms exist for reporting safety concerns.
| Code explicitly addresses this requirement. |
| | Code does not explicitly address this requirement. |
| | | Code explicitly addresses this requirement. |
| #9 Mobile providers should implement mechanisms for reporting safety concerns.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #10 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #11 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #12 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #13 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #14 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #15 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #16 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #17 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |
| #18 Mobile providers should ensure that their own-brand commercial content is classified in a similar way to that of third party content.
| Code explicitly addresses this requirement. |
| | Code does not specifically address this requirement. |
| | | Code explicitly addresses this requirement. |

Implementation Report
PricewaterhouseCoopers
May 09
<table>
<thead>
<tr>
<th>Country</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Germany</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Greece</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Hungary</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Ireland</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Italy</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Latvia</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement in terms of ensuring information distribution</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
</tr>
</tbody>
</table>

As of the point of preparation of our report, there is not yet an industry consensus on the drafting of a national code in Luxembourg. Signatory operators have contributed considerably during the preparation of the framework, while drafting a national code through a national code. Our assessment of compliance will therefore be based solely on the framework, with a view to bringing about the necessary framework, rather than to an industry consensus.

Not relevant to code

As at the point of preparation of our report, there is not yet an industry consensus on the drafting of a national code in Luxembourg. Signatory operators have contributed considerably during the preparation of the framework, while drafting a national code through a national code. Our assessment of compliance will therefore be based solely on the framework, with a view to bringing about the necessary framework, rather than to an industry consensus.
<table>
<thead>
<tr>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code does not explicitly address this requirement</th>
<th>Code does not explicitly address this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code explicitly addresses this requirement</th>
<th>Code does not explicitly address this requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement</td>
<td>Code does not explicitly address this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement</td>
</tr>
<tr>
<td>Code does not explicitly address this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement</td>
<td>Code does not explicitly address this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code explicitly addresses this requirement</td>
<td>Code does not explicitly address this requirement</td>
</tr>
<tr>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
</tr>
<tr>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
</tr>
<tr>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
</tr>
<tr>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
<td>Not relevant to compliance</td>
</tr>
</tbody>
</table>

Implementation Report
PricewaterhouseCoopers
May 09
Appendix 5: Reproduction of Operator Implementation Questionnaire

European Framework for Safer Mobile Use by Younger Teenagers & Children

Operator Implementation Questionnaire
Confidentiality and distribution of responses

This questionnaire has been prepared by PricewaterhouseCoopers LLP ("PwC") on behalf of GSMA Europe, in order to assist in an implementation review for the European Framework for Safer Mobile Use by Younger Teenagers and Children ("the Framework").

Several questions have been included that go beyond the basic scope of the requirements of the Framework. These questions are grouped under the heading of "additional voluntary procedures", and are intended to establish a fuller understanding of the many and varied ways in which mobile network operators ensure their compliance with the Framework, and are not intended to represent an endorsement or recommendation of any of the practices or mechanisms that may be mentioned.

All responses received will be collected by GSMA Europe but provided to PwC for review. The data collected will be consolidated into a report to be issued to GSMA Europe.

In the report, specific responses will not be connected to individual operators nor used as a means of ranking individual activities or procedures which differ from those used by other European operators. The data will be collated and assessed in a confidential manner and without prejudice on a national basis, and our opinions developed on the same basis, without revealing the specific responses of correspondents.

The final report will be made public and distributed by GSMA Europe to further parties, including, but not limited to, relevant EU stakeholders such as the European Commission.
Relevant definitions

**The Framework** – The European Framework for Safer Mobile Use by Younger Teenagers & Children. Also known as the “Safer Mobile Framework”.

**National Code** – A translation of the requirements of the Framework into a national code, taking into account the circumstances of your national market.

**Corporate policy** – An statement of policy or standard working practice for your organisation in relation to providing safer mobile use for younger teenagers and children. This may be separate from, and parallel to, any national or industry-generated codes of conduct, and might be in the form of a group policy applied in all regions where the group operates. In this case, the phrase refers to the policy or practice as far as it is relevant to your country of operation.

Where no national code of conduct exists and your organization is a signatory to the Framework, it is likely that such a corporate policy or standard working practice will have been created to satisfy the requirements of the Framework. In such cases, questions that do not specifically refer to either corporate policies or national codes should be answered based on whatever policies / standard practices exist within your country of operation.

**Commercial content** – Any content provided by commercial content providers to mobile customers. This includes pictures, video clips, mobile games, music, sounds and experiences such as gambling. It does not include content accessed via the Internet, where mobile operators are providing only the connectivity.

**Adult content** – Commercial content of an erotic or sexually explicit nature, or content such as gambling which requires the user to be of a certain age (i.e. viewed as an adult) by law in the country of your operations.

**Harmful content** – Commercial content which is not illegal (see below) but may nonetheless be inappropriate for the age or level of vulnerability of certain customers. Such content may be harmful to the mental or physical well-being of the user either through disrupting their normal social development (by advocating violence, substance abuse, discrimination or other harmful / illegal activities) or through enabling the victimisation, manipulation or abuse of the viewer. This classification is therefore extremely subjective. The classification of content as harmful (as opposed to adult) is entirely voluntary and will not be done by all operators, but may be undertaken by some companies or non-governmental organisations in order to provide different levels of content access controls or guidance to customers.

**Illegal content** – What is considered to be illegal varies from country to country, and is defined by the applicable national law. This term therefore refers here to content which is deemed illegal according to the laws and statutes of the country of your operations.

**Classification system** – Any process through which commercial content is assessed to identify whether it meets the criteria of one of the above categories (adult, illegal or harmful) and is then classified as such for the purposes of setting distinct access controls for the different categories.
**Branded content** – Commercial content that is sold under your own brand name, whether on your own network or through other media.

**(Contracted) Third party content providers** – Any providers of commercial content or services with whom your organisation has contractual agreements, under which they provide you with content that is sold or made available through your network.

**Access controls** – Any mechanisms used to prevent unrestricted access to commercial content, or to ensure that content is only made available to people of sufficient age or maturity for it not to be harmful to them (see above). This may include technological, physical or monitoring mechanisms, such as barring, PIN controlled access, subscription only services, age verifications and so on.
General Questions

Name of your organisation:

Country of operation:

Number of employees:

Turnover in FY07 or FY07/08:

1 - At what age are users considered by law to become adults in your country of operation (e.g. 18 years)?

2 - Are you currently a signatory of a national code of conduct (or equivalent) for mobile phone operators and content providers in your country of operation?

☐ Yes

☐ No

If yes, please provide the name of the code and the date of signature:

3 - What is the planned date of full implementation for this national code? Please specify any relevant dates / timeframes for past or future implementation where relevant.

4 - Does (or will) this national code specifically contain policies designed to ensure safer mobile use by younger teenagers or children who may be considered vulnerable to certain content?

☐ Yes

☐ No
5 - Does specific legislation exist in your country that requires certain standards of behaviour or compliance from mobile network operators to ensure the safety of users and/or the appropriateness of content, or legislation specifically relating to the protection of customers under a specific age?

☐ Yes

☐ No

If yes, please provide details of the relevant legislation for reference if possible:

........................................................................................................................................................................

........................................................................................................................................................................

........................................................................................................................................................................

........................................................................................................................................................................
Part 1 –Classification of Commercial Content

Framework area: Classification of Commercial Content

#9 Mobile operators must adopt a national system for classifying mobile commercial content that reflects approaches in existing national media with at least 2 categories (‘adult/18’ and ‘other’). Aim to reuse national classifications wherever possible, so customers experience the same system of classification whether they are using mobile or non-mobile media.

#10 Apply the classification system in #9 above to mobile operators’ own content.

6 - Is a classification system applied to your own-brand commercial content that is able to distinguish adult content from other content?

☐ Yes
☐ No

If not, when do you expect to introduce such a system?

________________________________________________________________________________________________________________________________________________________________________________________________________________________

6a - Please briefly outline the process through which you determine how content is to be classified:

________________________________________________________________________________________________________________________________________________________________________________________________________________________

________________________________________________________________________________________________________________________________________________________________________________________________________________________

________________________________________________________________________________________________________________________________________________________________________________________________________________________

7 - Does this classification system and its criteria reflect the approach used in your country for other media (e.g. photography / pictures in magazines or press, movies, television programmes, computer games)?

☐ Yes
☐ No

If no, please specify why not:

________________________________________________________________________________________________________________________________________________________________________________________________________________________

________________________________________________________________________________________________________________________________________________________________________________________________________________________
8 - Where you offer branded adult content, have these classification systems been applied to all your current adult content in order to separate it from other content?

☐ Yes

☐ No

If not, when do you expect that it will be applied to separate this content?

----------------------------------------------------------------------------------------------------

Additional voluntary procedures

9 - If you use further classification categories that extend beyond “adult” and “other”, please outline the categories that you use. (If you apply different systems of classification for different content or services, please specify for each different system used.)

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------

10 - Please briefly outline your response mechanism if any exceptions or errors in classification relating to your branded content are identified, how such errors would usually be identified, and any means which you might have in place to resolve this. If it is possible to provide an average time for this response, please state it.

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------
11 - Have these classification systems been applied to all current content acquired from contracted third party service providers?

- Yes
- No

If not, when do you expect that they will be applied to all content?

………………………………………………………………………………………………………………………….

11a - Is the same system of classification applied for your own branded content and content offered by contracted third party service providers?

- Yes
- No

If no, please explain in detail the differences between the classification systems applied and how you ensure that the “adult” classification is consistent between the two.

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

12 - Where adult content or services on your network are provided by contracted third party content providers, do you ensure that your contracts with them specify that such material should be classified according to such a system?

- Yes
- No

If no, when do you expect to implement such arrangements, and how do you currently ensure that the content supplied by such content providers is in line with your classification system?

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
13 - If any exceptions or errors in classification are identified relating to content provided by contracted third party suppliers (e.g. items of adult content for sale that are not correctly classified by the third party), do you actively attempt to inform the appropriate persons / organisations to ensure that the classifications are corrected?

☐ Yes
☐ No

Please briefly outline how such errors would usually be identified, and any means which you might have in place to facilitate this:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

14 - Do the third party content providers retain any rights or abilities to edit or add to content after its initial classification / acceptance?

☐ Yes
☐ No

If yes, is it possible for these changes to be made without review / acceptance of a new classification by yourselves?

☐ Yes
☐ No

Additional voluntary procedures

15 - How do you ensure that users are made aware of the classification or nature of any content they might request that is considered adult or harmful (e.g. warning page for online content, clearly visible signs on advertising or packaging for separately purchasable content)?

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
Part 2 – Access controls

16 - Do you offer adult content or services to users of your network under your own brand?
☐ Yes
☐ No

16a - If yes, do you offer means for restricting / blocking access to this adult content for users of your network?
☐ Yes
☐ No

If no, when do you intend to introduce such a system?

Framework area: Access Control Mechanisms
#1 Commercial adult content or services will not be offered by mobile operators without providing effective access controls.

Framework area: Access Control Mechanisms
#2 Access controls should also be applied over time to third party content / services that are supplied by commercial partners (including premium rate services).

17 - Do you offer adult content or services created by contracted third party content providers to users of your network?
☐ Yes
☐ No

17a - If yes, do you offer means for restricting / blocking access to this adult content for users of your network?
☐ Yes
☐ No

If no, when do you intend to introduce such a system?

Additional voluntary procedures

18 - In order to ensure that usage of your mobile devices is appropriate for the age / maturity of the user, do your access controls over content (whether produced by yourselves or by third parties) rely upon:

☐ Default handset-specific settings?

☐ Default user account configurations (e.g. content restrictions set by SIM card)?

☐ Sensible / monitored use by parents / guardians in setting the right controls?

☐ Combination of the above / other (please specify):

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................

19 - Do you perform customer identity and age verification checks on purchase of a device or contract to verify (as far as possible) whether the purchaser is a legal minor and that appropriate controls are therefore applied as far as necessary?

☐ Yes

☐ No

If yes, please specify the type of verification required (e.g. credit cards, reference to original customer data):

........................................................................................................................................................................
........................................................................................................................................................................

19a - Do you perform checks to verify (as far as possible) whether the device or contract is intended for use by a legal minor and that appropriate controls are therefore applied as far as necessary?

☐ Yes

☐ No

If yes, please briefly outline how this is achieved:

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
Framework area: Access Control Mechanisms

#3 Mobile network operators offer parental solutions to customise access based on what they believe will be commercially successful / best meet customers' needs.

20 - Please briefly outline what access controls mechanisms you currently offer to customers, or any mechanisms you plan to introduce, along with their planned implementation dates:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

Additional voluntary procedures

21 - Are any of these access controls or other restrictions that you offer customisable by the user on purchase or at a later date?

☐ Yes
☐ No

If yes, please briefly outline what the configurable options are:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
21a - By what means are users able to customise controls or request that controls be applied / changed / removed (please select all that apply)?

- Requesting change from salesperson upon purchase of device / contract
- Online application
- Call to customer services or equivalent
- Written application
- Disclaimer / confirmation of age when adult content is requested for first time
- Changing configuration of device
- Other (please specify): …………………………………………………………………………………………………………………

21b - Do you perform (or do you obtain from third parties) any age / identity verification checks when changes are requested to these customisable access control settings (e.g. removal of controls)?

- Yes
- No

If yes, please specify the type of verification required (e.g. credit cards, reference to original customer data)

………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………

22 - Are users actively informed about how to customise any access control options when they purchase a device / contract from you?

- Yes
- No
22a - If yes, please select all the means by which this is achieved:

☐ Documentation provided with product / contract on purchase
☐ Required presentation by salesperson completing sale
☐ Displays / leaflets positioned prominently in stores
☐ Prominent notifications or pop-ups on website
☐ Notification by email / on-screen statement / other means for online purchases
☐ Users are informed of other means of gaining this information (hotlines, websites, etc)
☐ Other (please specify): ...........................................................................................................................

23 - Is the default setting for your devices / accounts to have certain access controls enabled (i.e. preventing access to adult content) until it is specifically requested that they be removed?

☐ Yes
☐ No

If yes, please briefly outline what the default controls settings are:

................................................................................................................................................................
................................................................................................................................................................
................................................................................................................................................................
................................................................................................................................................................
................................................................................................................................................................

23a – Are these default settings applied in the same way for new customers and for existing users entering into a new contract?

☐ Yes
☐ No

If no, please briefly outline the differences in default settings and how these are controlled (i.e. what customer identity and age verification checks are applied to existing users entering into a new contract):

................................................................................................................................................................
................................................................................................................................................................
................................................................................................................................................................
................................................................................................................................................................
24 - Do you actively monitor or review the effectiveness of your access control systems in any way to ensure that they are achieving the desired safety for users?

☐ Yes

☐ No

If yes, please outline briefly your procedures in place for such reviews and their frequency:

....................................................................................................................................................
....................................................................................................................................................
....................................................................................................................................................
....................................................................................................................................................
....................................................................................................................................................

If no, do you have a means for customers to report problems with access controls or security settings (e.g. technical problems)?

☐ Yes

☐ No

Please outline what help or reporting methods are available to customers in this area:

....................................................................................................................................................
....................................................................................................................................................
....................................................................................................................................................
....................................................................................................................................................
....................................................................................................................................................
Part 3 – Fighting illegal content

Framework area: Fighting illegal content on mobile community products or the internet
#13 Continue to work with law enforcement regarding the reduction or elimination of illegal child images.

25 - Do you proactively communicate with local or national law enforcement agencies to report illegal child abuse content if you become aware of it, whether on your portal or on the internet?

☐ Yes
☐ No

If yes, indicate the name of the relevant authority and the mechanism and frequency of communication as relevant:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

Framework area: Fighting illegal content on mobile community products or the internet
#14 Support national authorities, for example by working through the local INHOPE hotline network or equivalent, in enabling the reporting of illegal child images by customers.

26 - Do you provide a specific means for customers to report illegal child abuse content on your portal or on the internet?

☐ Yes
☐ No

If no, when do you intend to introduce such a system?

………………………………………………………………………………………………………………………….
26a - If you already have a means for customers to report illegal content to you, please outline the reporting methods available:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

26b - Do you support or promote any hotline(s), websites or other means for reporting illegal child abuse content on the Internet that may be available in your country?

☐ Yes
☐ No

If yes, please outline the way in which you do so:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

Framework area: Fighting illegal content on mobile community products or the internet

#15 Support national notice and take-down approaches by removing illegal child images from the mobile operators’ own servers or by blocking access to such images when hosted on other servers. Work in liaison with law enforcement or other appropriate authorities. Support their creation where they do not exist.

27 - Do you have documented notice and take-down procedures in place in your organisation?

☐ Yes
☐ No

28 - Please briefly outline the steps your organisation would take if illegal content were discovered on your portal, either within your own content or that provided by third parties:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
29 - Apart from any national legislation regarding illegal content, do any other bodies or organisations exist in your country which focus on monitoring and/or preventing illegal content?

☑ Yes
☑ No

If yes, please provide names and some idea of their purpose or activities:
...........................................................................................................................................................................................
...........................................................................................................................................................................................
...........................................................................................................................................................................................

29a - Do you proactively communicate with these or other international associations (for example INHOPE) to report illegal content on your portal or on the internet?

☑ Yes
☑ No

If no, do you intend to begin working with such organisations and when do you expect to do so?
...........................................................................................................................................................................................
...........................................................................................................................................................................................

29b - If no such bodies or associations exist in your country of operation, please outline any involvement you may have in encouraging or supporting their creation:
...........................................................................................................................................................................................
...........................................................................................................................................................................................
...........................................................................................................................................................................................

Additional voluntary procedures

30 - Do you track the speed with which you respond to reports of illegal content from customers?

☑ Yes
☑ No

If yes, please state the average length of time for a response if possible (e.g. removal of the offending content, reporting to the authorities):
...........................................................................................................................................................................................

31 - Please outline briefly any additional procedures in place within your organisation to ensure that you comply with your responsibilities under local and/or international laws with regard to illegal content (e.g., identifying and restricting violent sexual content, content involving sex with animals or any other content which may be illegal in your country):

................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
................................................................................................................................................
Part 4 – Raising awareness

Framework area: Raising Awareness and Education
#4 Mobile operators should provide information to customers on safer mobile use.
#7 The main target for awareness-raising should be customers. Mobile operators may also work through organisations such as the INSAFE network.

32 - Do you currently run any campaigns, produce educational literature, or have active involvement in any other activities with the aim of increasing public awareness of safer use of mobiles or the dangers of certain internet content to the well being (either physical or mental) of vulnerable age groups?

☐ Yes
☐ No

If yes, please select the methods which you use from the list below, or briefly outline the nature of these campaigns if not listed:

☐ Documentation provided with product / contract on purchase
☐ Required presentation by salesperson completing sale
☐ Displays / leaflets positioned prominently in stores
☐ Prominent notifications or pop-ups on website
☐ Notification by email / on-screen statement / other means when product / contract is purchased online
☐ Users are informed of other means of gaining this information (hotlines, websites, etc)
☐ Involvement with other organisations focused on raising awareness (please specify the organisations): ......................................................................................................................................
☐ Other (please specify): ..................................................................................................................................

32a - If you do not currently do any of the above, do you have a plan or schedule for initiating such awareness-raising campaigns, producing literature or other activities in the near future?

☐ Yes
☐ No
32a cont. - Please briefly outline the nature and planned timings of these activities where relevant, and whether they will be run independently or in collaboration with other organisations:

........................................................................................................................................................................

........................................................................................................................................................................

........................................................................................................................................................................

Framework area: Raising Awareness and Education
#5 Parents talking to children about mobile use and what to do in the event of concerns should be a top-level message.

33 - Which of the following messages do / will any such awareness-raising campaigns in which you are involved explicitly focus on (please select all that apply)?

☐ The potential dangers of certain multimedia content to the well being (either physical or mental) of younger teenagers or children

☐ The role of parents / legal guardians / teachers in informing younger teenagers & children of such dangers

☐ The role of parents / legal guardians / teachers in actively protecting younger teenagers & children from such content through preventing access, monitoring usage, etc.

☐ The organisations in existence for users to report any concerns about illegal or unsuitable content

☐ The functionality / controls available to users of your services to ensure that younger teenagers & children are using their mobile devices safely and appropriately

☐ Ways of reacting to and preventing abuse of mobile phones (e.g. bullying by phone, inappropriate use of mobile phone cameras)

☐ Other (please specify):

........................................................................................................................................................................
34 - Do you have in place a system to allow customers to report safety concerns, such as fears over the abuse or misuse of mobile phones by younger teenagers or children?

☐ Yes

☐ No

If yes, please outline the key features of this system and ways in which customers are able to report their concerns:

................................................................................................................................................................

................................................................................................................................................................

................................................................................................................................................................

................................................................................................................................................................

................................................................................................................................................................

................................................................................................................................................................

Framework area: Raising Awareness and Education

#6 Mobile operators should provide customers with details of how to report safety concerns. Customer services should be equipped to handle and forward customer reports to the appropriate authority.
Part 5 – Further voluntary measures beyond the requirements of the Framework

35 - Do you actively assess commercial content hosted on your own servers (either branded content or content from contracted third party content providers) on a regular basis in order to ensure that illegal or potentially harmful content is not accessible through your network?

☐ Yes
☐ No

If yes, please outline briefly your procedures in place for identifying and responding to such content within your proprietary content or on your servers, and their frequency:
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

36 - Where your organisation has any means in place to actively identify and block content from third parties or on the internet (either because it is illegal or harmful, or in order to prevent children viewing adult content), please outline the nature and extent of these controls:
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
37 - Where chat rooms or other real-time communication forums are available on your network, are these able to be held without moderation or monitoring?

☐ Yes
☐ No

If yes, please clarify whether any are monitored and how the monitored ones would be selected. If any monitoring is provided, please outline briefly the way in which interactions are monitored:

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….

38 - Please provide a very high-level summary of any additional areas, controls or mechanisms that you may have in place to ensure safer mobile use by younger teenagers or children that arise from corporate policies, standard working practices or additional local legislation / regulation other than national codes (e.g. restrictions on marketing to children, content selection policy):

………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
………………………………………………………………………………………………………………………….
European Framework for Safer Mobile Use by Younger Teenagers & Children
Implementation Questionnaire

39 - Do you actively seek to review / refine your policies (both internal or those relating to compliance with any national code) as regards safer usage of mobile devices by younger teenagers and children on a regular basis?

☐ Yes

☐ No

If yes, please briefly outline how this is achieved, or what resources are allocated to this:

........................................................................................................................................................................

........................................................................................................................................................................

40 - When developing any relevant corporate policies, reviewing national codes, or establishing your organisation’s working practices, please outline the main bodies, documents or guidance to which you may have referred (e.g. practices of other operators, national codes of conduct, national legislation, civil bodies or non-governmental organisations):

........................................................................................................................................................................

........................................................................................................................................................................

........................................................................................................................................................................
41 – Is there any extent to which staff within your organisation are provided with incentives to seek out or improve ways to improve safety of mobile use for customers (e.g. bonuses or salaries linked to implementing new controls, key performance indicators about safety used to determine performance of departments)?

☐ Yes
☐ No

If yes, please briefly describe how this is achieved:

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................

42 – Please give a brief idea of the nature of any potential consequences / reactions that may arise if an operator in your country failed to meet the requirements of the national code, where relevant:

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................

Thank you for taking the time to respond. Your input is extremely valuable.

If your organisation does have any form of corporate policy relating to safer mobile use or the protection of young teenagers and children, would you please return this questionnaire with a copy of this policy (or relevant extracts) if this is possible. This is purely for the purpose of providing a means of cross-reference and clarification for answers, and not in order to identify specific operators’ policies, as stated in the confidentiality details (page one).
Access control mechanisms

Requirement #1

Question: Do you offer adult content or services to users of your network under your own brand, and if so do you offer means for restricting / blocking access to this adult content for users of your network?

![Graph showing compliance against Framework Requirements by Country]

Requirement #2

Question: Do you offer adult content or services created by contracted third party content providers to users of your network, and if so do you offer means for restricting / blocking access to this adult content for users of your network?

![Graph showing compliance against Framework Requirements by Country]
Requirement #3

**Question:** Are any of the access controls or other restrictions that you offer customisable by the user on purchase or at a later date?

Raising awareness and education

Requirement #4

**Question:** Do you currently run any campaigns, produce educational literature or have active involvement in any other activities with the aim of increasing public awareness of safer use of mobiles or the dangers of certain internet content?

Requirement #5

All the operators who currently undertake awareness-raising activities, or intend to do so (83% in total - see requirement #4) stated that the explicit messages of their campaigns would contain some, if not all, of the below points:

- The potential dangers of certain multimedia content to the well being (either physical or mental) of younger teenagers or children
The role of parents / legal guardians / teachers in informing younger teenagers & children of such dangers
The role of parents / legal guardians / teachers in actively protecting younger teenagers & children from such content through preventing access, monitoring usage, etc.
The organisations in existence for users to report any concerns about illegal or unsuitable content
The functionality / controls available to users of mobile services to ensure that younger teenagers & children are using their mobile devices safely and appropriately
Ways of reacting to and preventing abuse of mobile phones

Requirement #6

Question: Do you have in place a system to allow users to report safety concerns, such as fears over the misuse of mobile phones by younger teenagers and children?

Requirement #7

This requirement is intended to promote cooperation between mobile operators and a variety of other organisations seeking to increase public awareness or safer internet use in different countries. We have therefore primarily considered the responses to question 32 in the questionnaire, as to whether operators specifically work / plan to work with any organisations to promote awareness of safer mobile use. However, we have also assessed whether the operators support / promote other third-party organisations in other capacities, including hotlines, websites or other international associations for reporting illegal content. This is summarised below.
Classification of commercial content

Requirements #9 & #10

Operators were asked whether they use or support a classification framework for their own-brand content that consists of two categories as a minimum: content suitable only for adult customers and other content. They were also asked whether this classification system reflects approaches used in other media in their country of operation. Where operators are using such a system, they can be seen to support it by default. The lack of any such system will also only be relevant where operators are offering content to which it is not applied.

Question: Do you apply a classification system to your own-brand content that is able to distinguish between “adult” and “other” content, and if so does this reflect the approach used for other media?
Requirement #11

Question: Do you offer any adult content from third-party suppliers, and if so is this content classified by yourself or is the supplier contractually obliged to classify it?

Fighting illegal content on mobile community products or on the internet

Requirement #13

Question: Do you proactively communicate with local or national law enforcement agencies to report illegal child abuse content if you become aware of it, whether on your portal or on the internet?
Requirement #14

Question: Do you provide a means for customers to report illegal child abuse content to you, or do you support or promote any hotlines, websites or other means of reporting child abuse content?

Requirement #15

Question: Do you proactively collaborate with local law enforcement or any other relevant national / international organisation to report illegal content?

Implementation, Stakeholder Consultation & Review

Requirement #17

For a summary of implementation of the Framework at a national level, please see the section of this report entitled “Adoption of the Framework into Codes of Conduct”.
Requirement #18

Question: Do you actively seek to review / refine your policies as regards safer usage of mobile devices by younger teenagers and children on a regular basis?