This deliverable carries out a first analysis of the legal and ethical principles pertaining to the EXPERIMEDIA project. This deliverable provides an initial legal analysis of the different scenarios and experiments of EXPERIMEDIA and it should be perceived as an introductory and complementary document to the Ethics Review Reports that are to be composed in close collaboration with the EXPERIMEDIA Ethics Advisory Board. The legal analysis focuses on the explanation of the most important legal concepts that will inevitably impact on the scenarios and experiments, regardless how they dynamically change during the project. The most important aspects that have to be taken into account refer mainly to privacy and data protection, media regulation and Intellectual Property Rights.
<table>
<thead>
<tr>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial release</td>
</tr>
<tr>
<td>1.1</td>
<td>Creative Commons information added; other minor updates</td>
</tr>
<tr>
<td>1.11</td>
<td>Updated front page and metadata table</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Executive Summary................................................................. 4

2. Introduction .............................................................................. 5
   2.1. EXPERIMEDIA and its ethical, legal and regulatory framework .... 5
   2.2. Experiments ......................................................................... 5
       2.2.1. Schladming .................................................................. 5
       2.2.2. CAR .......................................................................... 6
       2.2.3. FHW .......................................................................... 6

3. Content Regulation..................................................................... 8
   3.1. Introduction ......................................................................... 8
   3.2. Scope of the TWF Directive .................................................. 8
   3.3. Scope of the AVMS Directive ............................................... 9
       3.3.1. Audiovisual media service ......................................... 9
       3.3.2. Linear versus non-linear services .............................. 13
       3.3.3. Media service provider ............................................. 13
   3.4. Two-tiered regulation .......................................................... 14
       3.4.1. Introduction ............................................................... 14
       3.4.2. Basic tier obligations ................................................ 15
       3.4.3. Rules applicable to on-demand audiovisual media services 15
       3.4.4. Rules applicable to linear audiovisual media services ...... 15
   3.5. Technology-neutrality ......................................................... 19

4. Copyright .................................................................................. 21
   4.1. Introduction ......................................................................... 21
   4.2. No harmonization .................................................................. 21
   4.3. Public domain ....................................................................... 23
   4.4. Copyright holder ................................................................... 23
   4.5. Exceptions ........................................................................... 23
   4.6. Terms of Use ......................................................................... 24
   4.7. Copyright and sports events .................................................. 24
       4.7.1. Sports events: copyright protected or not? .................... 24
   4.8. UGC and sports events ........................................................ 26
   4.9. Open content licenses – Creative Commons ......................... 28
       4.9.1. Introduction .................................................................. 28
4.9.2. Creative Common (CC) Licenses ........................................................................... 29
5. Privacy policy framework .......................................................................................... 34
  5.1. Introduction ........................................................................................................... 34
  5.2. General privacy regulation .................................................................................. 34
      5.2.1. Directive 95/46/EC ................................................................................. 35
      5.2.2. Location based services ........................................................................... 52
      5.2.3. National privacy legislation ..................................................................... 53
      5.2.4. Review of Directive 95/46/EC ................................................................. 54
6. Liability issues ............................................................................................................ 57
  6.1. Liability of service providers ............................................................................... 57
      6.1.1. Introduction ............................................................................................... 57
      6.1.2. Mere conduit ............................................................................................. 57
      6.1.3. Caching ...................................................................................................... 58
      6.1.4. Hosting ....................................................................................................... 58
      6.1.5. No general obligation to monitor ............................................................... 59
  6.2. Liability under data protection regulations ......................................................... 60
7. Conclusion ................................................................................................................... 62
1. Executive Summary

The objective of this deliverable is to clarify the legal state of the art and rules applicable to the EXPERIMEDIA project and to ensure that the different experiments are compatible with the different regulatory frameworks. This deliverable provides an initial legal analysis of the different scenarios and experiments of EXPERIMEDIA. It comes as no surprise that the current legal framework will be challenged by the development of new services. The experiments of EXPERIMEDIA serve as tool to indicate where difficulties could arise. The methodological framework developed by EXPERIMEDIA (EAB, VIA, PIA) is intended to anticipate these risks.

The legal analysis focuses on the explanation of the most important legal concepts that will inevitably impact on the scenarios and experiments, regardless how they dynamically change during the project. The most important aspects that have to be taken into account refer mainly to:

- privacy and data protection
- media regulation
- Intellectual Property Rights.

When the applicable legal framework is described and explained, it will be applied to the different experiments of EXPERIMEDIA.

Based on the issues identified in the analysis of the current legal frameworks, requirements are formulated in order to ensure compliance with these specific branches of law.

This deliverable should be perceived as an introductory and complementary document to the Ethics Review Reports that are to be composed in close collaboration with the EXPERIMEDIA Ethics Advisory Board (EAB).
2. Introduction

2.1. EXPERIMEDIA and its ethical, legal and regulatory framework

EXPERIMEDIA will develop and operate a unique facility that offers researchers what they need for large-scale Future Media Internet experiments. Experiments within EXPERIMEDIA are expected to explore Future Internet systems targeting enhanced and contextualised user experience, immersive and interactive media technologies (co-creation and collaboration tools, augmented reality, etc), content production, distribution and delivery platforms (content objects, dynamic adaptation and aggregation, hybrid delivery/return infrastructures, etc), and new social interaction models. With such objective a number of legal questions arise.

The aim of this deliverable is to describe the applicable legal framework and to evaluate the consequences for EXPERIMEDIA. It will also identify problems that could be encountered due to the current state of the regulatory framework. The main areas that have to be tackled to ensure compliance with the existing law focus around privacy and data protection, intellectual property rights and content regulation. The present deliverable provides an introduction to the subject, analysis of the relevant legislation and presentation of the legal requirements that will need to be adhered to throughout the EXPERIMEDIA project to ensure the legal compliance of the EXPERIMEDIA project.

The different experiments will be assessed against the current legislative framework, including:

- Content regulation
- Copyright regulation
- Data protection legislation
- Legal framework on liability

2.2. Experiments

In the first phase of EXPERIMEDIA, three driving experiments, led by the Venue partners, will be used to verify, validate and demonstrate the facility capabilities in preparation for the open calls. This includes augmented reality services and UGC at large-scale live events at Schladming, content production and delivery for high quality and 3D Internet-based remote sports analysis and training at CAR and shared, real-time, immersive and interactive cultural and educational experiences at FHW. Given that, throughout this document, the implications of the regulatory framework for EXPERIMEDIA and the different experiments will be highlighted, it is necessary that a short description of the different driving experiments is included in this deliverable.

2.2.1. Schladming

Schladming is a tourist place. Hence, the main objective for Schladming is to provide visitors and citizens services that improve the visitor experience and improve the quality of life. Both visitors as citizens should have all the information they need to have the best possible experience in Schladming available instantaneously. The experiment should support a smooth and satisfactory "customer journey" that starts when the visitor researches information about an event or vacation in Schladming, continues throughout all further phases including the actual stay at Schladming.
Schladming until the visitor leaves the place and shares his experiences with friends. A mobile application (or “app”) will be created, which allows visitors to experience the region and its activities in a modern and innovative way. The app will help visitors of the ski world championships find side events and help them see where "the party is on". The service should also connect fans and help them in getting together. In this scenario, Social Networking Sites are exploited as an interface between real-world and virtual information, and for location-sensitive real-time group messaging. Other technologies are "actuated" through the social interconnection of users. For example, users can initiate a video streaming service through their interconnection, and use it to communicate with each other. 3D capture points will be set up on standard routes for non-competitive skiing, where EXPERIMEDIA end-users can have a 3D snapshot of their interesting achievements taken. Visitors' mobile devices will allow them to immediately find the captured content that concerns them, and will be given further instructions how to view the content. In short, the experiment at Schladming is dealing with roaming individuals using mobile technology to organise and enhance their group experiences.

2.2.2. CAR
The aim of the second experiment, carried out at CAR, is to enhance the process of creating a new synchronized swimming choreography and improve the training sessions done by the team. Two groups of 7 members create their own choreography for the same music. Each group will present their ideas while the trainer is recording the movements and selecting the most interesting parts. The team assigns numbers to different parts of the music. The team knows that at a specific number they must have done a movement and reached a position with some part of their body, e.g. leg must be stretched. This numbers should appear on the screen while they watch the choreography. The choreography will be streamed. The video could be stored in a database in order to reuse it in the future. People of the team who are not able to attend the training also have access to the video from home and they can control remotely what the swimmers are watching on the television next to the swimming pool. In short, the experiment at CAR is focused on specific training sessions and interactions with their coaches; synchronization with media.

2.2.3. FHW
During the third scenario, a museum educator is physically located in Tholos at FHW. This museum educator is responsible for presenting and for navigating through the 3D movie about, for example, ancient ruins. A team of experts (e.g. historians and/or archaeologists that were actually involved in the excavation of the ruins) joins this educator. This team of experts may be geographically dispersed and are brought together and in contact with the museum educator and the audience in Tholos by using the EXPERIMEDIA facilities. The audience, while viewing the 3D movie, will be able to interact with the panel of experts (i.e. ask questions, make comments, express preferences, etc.) through their preferred social networking interface using smart-phones, laptops or tablet PCs.

During the presentation, the experts can send feedback to the audience and the museum educator either by answering questions in real time, or by texting answers. To facilitate this, the experts’ end-user application will be enhanced with a social network plug-in that will automatically collect and present to the archaeologist any relevant comments/questions coming
from the remote audience in Tholos. The feedback enhances the presentation by providing answers to directed questions regarding the visual content of Tholos in real time.
3. Content Regulation

3.1. Introduction


3.2. Scope of the TWF Directive

The scope of the TWF Directive was limited to television broadcasting services meaning “the initial transmission by wire or over the air, including that by satellite, in unencoded or encoded form, of television programmes intended for reception by the public. It includes the communication of programmes between undertakings with a view to their being relayed to the public. It does not include communication services providing items of information or other messages on individual demand such as telecopying, electronic data banks and other similar services”.

In the Mediakabel case, the Court of Justice was asked to interpret the notion of ‘television broadcasting’ in the light of the notion of ‘information society services’ (infra) and with a view to qualifying (semi-)interactive media services like (near-)video on-demand. The Court of Justice clarified that ‘a service comes within the concept of ‘television broadcasting’ [...] if it consists of the initial transmission of television programmes intended for reception by the public, that is, an indeterminate number of potential television viewers, to whom the same images are transmitted simultaneously. The manner in which the images are transmitted is not a determining element in that assessment’. "The exclusion of ‘communication services … on individual demand’ from the concept of ‘television broadcasting’ means that, conversely, the latter concept covers services which are not supplied on individual demand’. Hence, one of the key characteristics of television broadcasting is that the programmes are transmitted in a linear fashion, so that the content items are transmitted consecutively and can consequently only be received at the same time.

---

3 Art. 1 (a) of the TWF Directive.
3.3. **Scope of the AVMS Directive**

3.3.1. **Audiovisual media service**

The AVMS Directive applies to all audiovisual media services (AVMS). ‘Audiovisual media service’ is defined by Article 1(1)(a)(i)-(ii) of the AVMS Directive as “a service as defined by Articles 56 and 57 [ex 49 and 50] of the Treaty of the Functioning of the European Union which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes in order to inform, entertain or educate, to the general public by electronic communications networks”. An AVMS includes linear as well as non-linear services (infra). This definition consists of seven constituent elements:

3.3.1.1. **Economic service**

The reference to Articles 56 and 57 implies that the service must have an economic character and normally be provided for remuneration. Due to this first condition, non-economic activities which are not in competition with television broadcasting, such as private websites, blogs and services consisting of the provision or distribution of audiovisual content generated by private users for the purposes of sharing and exchange within communities of interest, are excluded from the scope of the AVMS Directive. However, websites that carry advertisements as their major source of income are audiovisual media services and thus must comply with the requirements of the AVMS Directive.

**MoreVideo – UGC productions**

MoreVideo is a technology for amateur UGC productions from multiple video sources. If the results of this production fulfil the 7 criteria, this content falls under the scope of the AVMS Directive. Given that UGC is often a non-economic activity, the ‘economic purpose’ criterion is not fulfilled.

3.3.1.2. **Editorial responsibility**

A service will only be classified as an AVMS when the service falls under the editorial responsibility of a media service provider. Editorial responsibility is defined in Article 1 (1) (c) of the AVMS Directive as “the exercise of effective control both over the selection of the programmes and over their organisation either in a chronological schedule, in the case of television broadcasts, or in a catalogue, in the case of on-demand audiovisual media services. Editorial responsibility does not necessarily imply any legal liability under national law for the content or the services provided”. The notion ‘editorial responsibility’ and ‘effective control’ should be further specified by the individual Member States. As a result, services providers that do not have effective control over the content and only give the possibility for the distribution and uploading of audiovisual content generated by private users (user-generated content) for the purposes of sharing and exchange within communities of interest are excluded from the scope of the AVMS Directive. Providers of YouTube or YouTube-like services do not actively select the content and do not control its organisation in a chronological schedule or a catalogue. They only offer a portal and platform to users to make audiovisual content of their own available to a wide

---

5 Recital 21 of the AVMS Directive.
6 Recital 25 AVMS Directive.

© Copyright KU Leuven and other members of the EXPERIMEDIA consortium 2012
audience. However, it would appear that they exercise at least some secondary control over the content of their sites. For example, they usually post a (minimum) code of conduct and have a policy of removing videos that have been flagged by the users of the community themselves as inappropriate or which infringe the copyright of others. As long as the intervention is ex post, acting upon complaints from users, and does not involve an active selection ex ante, such control is not considered as editorial responsibility in the sense of the AVMS Directive. Therefore, they do not exercise editorial responsibility within the meaning of the AVMS Directive.

**Schladming - User-generated video streaming and sharing**

Visitors of Schladming are stimulated to upload audiovisual content or pictures of their journey (user generated content - UGC) at Schladming on YouTube like or Facebook like services. The AVMS Directive only applies to economic services. Recital 21 of the AVMS Directive explicitly excludes UGC from the scope of the Directive. This implies that the content created by visitors or citizens of Schladming and shared via YouTube like or Facebook like services does not have to meet the obligations included in the AVMS Directive.

If Schladming would be providing such services, Schladming could not be classified as a media service provider, because it does not have effective control over the content and only give the possibility for the distribution and uploading of audiovisual content generated by private users. If Schladming would actively select the content and do control its organisation in a chronological schedule or a catalogue, it is not merely offering a portal for UGC. Given that the control is no longer limited to ex post control, but has become ex ante control, Schladming would be labelled as a media service provider and have to take into account the obligations of the AVMS Directive.

**MoreVideo – UGC productions**

MoreVideo as such does not fall under the scope of the Directive, because it only offers the technology/a tool. It does not have any editorial responsibility.

### 3.3.1.3. Principle purpose

For a service to be an AVMS, its principal purpose should be the provision of programmes. As indicated in recital 22, services where audiovisual content is merely incidental to the service and not its principal purpose, such as animated graphical elements, short advertising spots or information related to a product or non-audiovisual service, should be excluded from the definition. A travel agency showing a clip of a holiday resort on its website remains outside the

---


scope of the Directive, as the images are only provided incidentally to the service of selling holidays. Similarly, an advertising spot on the website of a car manufacturer, for instance, does not have to meet with the requirements of the AVMS Directive, because the distribution of the audiovisual content is not the principal purpose of the website. For the same reasons, gambling websites, online games and search engines, which show audiovisual content, but whose principal purpose is not to provide programmes in order to inform, entertain or educate the public could not be labelled as AVMS. By contrast, broadcasts devoted to gambling or games of chance are included in the notion of audiovisual media service.

**CREATOR technology**

If interactive games are created using the CREATOR technology, the AVMS Directive does not apply. If the game could we considered as an original work, the game could be copyright protected (infra).

3.3.1.4. **Programme**

The service must distribute programmes to be an audiovisual media service. A programme is defined in Article 1 (1) (b) of the AVMS Directive as “a set of moving images with or without sound constituting an individual item within a schedule or a catalogue established by a media service provider and the form and content of which are comparable to the form and content of television broadcasting. Examples of programmes include feature-length films, sports events, situation comedies, documentaries, children’s programmes and original drama”. Examples of programmes include feature-length films, sports events, situation comedies, documentaries, children’s programmes and original drama. The notion of programme should be interpreted in a dynamic way, taking into account developments in television broadcasting.

Blogs that do not primarily provide moving images, but mainly offer text or pictures, are not considered to be audiovisual media services. For example, a blog put up by the local village football team, even if it is sponsored by a local firm, would not have to comply with the obligations of the AVMS Directive. Because the term ‘audiovisual’ refers to moving images with or without sound, it includes silent films but does not cover audio or radio transmissions.

Even though the principal purpose of an audiovisual media service should lie in the provision of programmes, the definition of such a service also covers text-based content which accompanies programmes, such as subtitling services and electronic programme guides, but not stand-alone text-based services. As a result, the AVMS Directive does not apply to electronic versions of newspapers and magazines or to websites without any audiovisual media content.

The AVMS Directive only covers “television-like” services, which reflects aspects of competition and user expectations: if the service competes for the same audience as television broadcasts, and

---

11 Recital 22 AVMS Directive.
12 Recital 24 AVMS Directive.
14 Recital 23 AVMS Directive.
15 Recital 23 AVMS Directive.
16 Recital 28 AVMS Directive.
the nature and the means of access to the service would lead the user to reasonably expect regulatory protection, the service will be considered as “television-like”.

**FHW – 3D movie**

If FHW would decide to put the different movies in a schedule on a website, these movies could be grasped by the notion ‘programme’. However, FHW does probably not have to take into account the obligations as described in this chapter. In fact, the question that needs to be answered is whether the ‘principal purpose’ of FHW is the provision of programmes (supra). The principal purpose of FHW (its mission) is the preservation and dissemination of Hellenic history and tradition, the creation of an awareness of the universal dimension of Hellenism and the promotion of its contribution to cultural evolution. In order to achieve this mission, FHW organises *inter alia* conferences, seminars, film projections, the production of printed publications, as well as visual and sound recordings. As a result, the provision of programmes is not the principal purpose of FHW.

3.3.1.5. **Inform, entertain and educate**

An audiovisual media service must be intended to inform, entertain and educate the public. Commercial websites featuring audiovisual content using webcams (e.g. snow or road traffic conditions) would not be considered as informing, entertaining or educating, because there is no editorial control over the audiovisual content.

3.3.1.6. **The general public**

The AVMS Directive covers only ‘mass media’, which are intended for reception by, and which could have a clear impact on, a significant proportion of the general public. Any form of private correspondence, such as emails sent to a limited number of recipients, are excluded from its scope. As images must be delivered to the general public for a service to be an audiovisual media service, audiovisual services offered only to persons present on the premises of certain companies (such as a department store or metro station) are not intended to be included as they are not provided to the general public.

**FHW – 3D movie**

The movie that is shown in Tholos does not reach the general public. In contrast, this audiovisual service is offered only to persons present in Tholos. As a result, these services do not fall under the scope of the AVMS Directive.

---

17 Recital 24 AVMS Directive.
19 Recital 21 AVMS Directive.
20 Recital 22 AVMS Directive.
3.3.1.7. Electronic communications networks

The type of network or the transmission method used for the delivery of the service is not a relevant criterion in determining if a service is an audiovisual media service. As a result, the AVMS Directive abandons the idea of regulating different platforms separately and instead creates a platform-neutral framework. This implies that not the transmission method, but the nature of the service should determine the type of regulation that is applicable. It is thus irrelevant whether an AVMS is delivered via cable, air, satellite or ADSL, the same rules apply (infra).\(^\text{22}\)

3.3.2. Linear versus non-linear services

The scope of the TWF Directive was broadened, with the adoption of the AVMS Directive, to include all audiovisual media services, both (traditional) broadcast services and on-demand services. However, the AVMS Directive still makes a distinction between these two categories, not only for definitional reasons, but also in terms of applicable rules: only minimum rules apply to the on-demand services, while an additional tier of stricter rules applies to the linear services. This system is called ‘graduated regulation’ or a ‘two-tiered approach’ (infra).

The AVMS Directive uses ‘television broadcasting’, ‘television broadcast’ and ‘linear audiovisual media service’ as synonyms and defines this notion as “an audiovisual media service provided by a media service provider for simultaneous viewing of programmes on the basis of a programme schedule”.\(^\text{23}\) In short, the media service provider decides upon the moment in time when linear services, such as classic television, near-video-on-demand\(^\text{24}\) and streaming, are transmitted and establishes the programme schedule. In other words, it is a push service, i.e. the programmes are pushed to the viewers who do not have any influence at all on the content of the broadcasting and the time they are displayed.\(^\text{25}\) In contrast to the linear television broadcasting, the non-linear services are pull services, i.e. the user decides upon the moment in time when a specific programme is transmitted. In short, the difference between linear and non-linear services ultimately depends upon who decides when a specific programme is transmitted and whether fixed schedules exist.\(^\text{26}\)

3.3.3. Media service provider

The ultimate addressees of the obligations contained in the AVMS Directive are the media service providers, who are the natural or legal persons with editorial responsibility for the choice of the audiovisual content of the audiovisual media service and who determine the manner in which it is organised.\(^\text{27}\) This excludes natural or legal persons who merely transmit content for which the editorial responsibility lies with third parties.\(^\text{28}\)

\(^{23}\) Art.1(1)(e) AVMS Directive.
\(^{24}\) Near-video-on-demand is a service not provided on individual demand, because the recipient does not individually demand the transmission data. Thus, the transmission is not on demand, it is accessible only on demand (O. Castendyk & L. Woods (2008). Article 1 TWFD. In O. Castendyk et al. (Eds.). *European media law.* Alphen a/d Rijn: Kluwer law international, 288).
\(^{27}\) Art.1(1)(d) AVMS Directive.
\(^{28}\) Recital 19 AVMS Directive.
Schladming - Planai TV

Planai TV is the broadcaster of the extended Schladming region. It can be accessed via cable, over-the-air and the Internet. Planai TV could be labelled as a media service provider, because it has the editorial responsibility for the choice of the audiovisual content and determines the manner in which it is organised. The content that is offered by Planai TV is AVMS, because all 7 criteria of the definition are met. This implies that Planai TV has to comply with all the obligations included in the AVMS Directive (infra). However, the audiovisual content broadcast by Planai TV webcams, such as snow or road traffic, will not have to meet the obligations included in the AVMS Directive, because (as indicated by the Council of the European Union) there is no editorial control over this audiovisual content.

3.4. Two-tiered regulation

3.4.1. Introduction

Although non-linear services are also covered by the new AVMS Directive, the European legislator considered that a horizontal approach to content regulation would only be effective if linear and non-linear services follow a two-tier regulation system. This graduated regulation implies that a basic tier of rules applies to all AVMS and that linear services have to meet additional obligations.

This different treatment has been introduced because of the difference in the degree of choice and control the user can exercise and by the different impact the services have on society. Compared to non-linear services, the user has no real impact on the content of linear television schedules. The decision about what to see and when to see is vested with the broadcaster and content is received in real time as it is being disseminated. Thus, the viewer is a passive consumer of information. Furthermore, it is argued that non-linear services have less impact on society, because the content is not viewed simultaneously by the public as viewers themselves determine the time of transmission. This difference justifies the light-touch regulation for non-linear services.

When television broadcasting or television programmes are also offered as on-demand services by the same media service provider, the requirements of the AVMS Directive are deemed to be met by the fulfilment of the requirements applicable to the television broadcast (i.e. linear transmission). However, where different kinds of services are offered in parallel, but are clearly separate services, the relevant provisions of the AVMS Directive apply to each of the services concerned.

30 Recital 58 of the AVMS Directive.
33 Recital 58 of the AVMS Directive.
34 Recital 27 AVMS Directive.
3.4.2. Basic tier obligations
All audiovisual media services, both linear and on-demand, are subject to the following minimum requirements.

3.4.2.1. Transparency and information obligation (Art.5. Recital 45)
Media service providers shall make easily, directly and permanently accessible to the recipients of the service at least the following information: the name of the media service provider, the geographical address at which the media service provider is established, the details of the media service provider (including its electronic mail address or website).

3.4.2.2. Prohibition of incitement to hatred (Art.6)
AVMS must not contain any incitement to hatred based on race, sex, religion or nationality.

3.4.2.3. Accessibility for people with a visual or hearing disability (Art.7. Recital 46)
Media service providers should ensure that their services are gradually made accessible to people with a visual or hearing disability (sign language, subtitling, audio description and easily understandable menu navigation).

3.4.2.4. Cinematographic works (Art.8)
Member States must ensure that media service providers under their jurisdiction do not transmit cinematographic works outside periods agreed with the rights holders.

3.4.2.5. Basic requirements for audiovisual commercial communication (Art. 9).
Minimum requirements apply to commercial communications on linear and non-linear services.

3.4.3. Rules applicable to on-demand audiovisual media services

3.4.3.1. Protection of minors (Art. 12, Recital 60 & 62)
Member States must take appropriate measures to ensure that on-demand AVMS provided by media service providers which might seriously impair the physical, mental or moral development of minors are only made available in such a way that ensures that minors will not normally hear or see such services (e.g. personal identification numbers (PIN codes), filtering systems or labelling). Prior verification by public bodies it not required.

3.4.3.2. European works (Art. 13, Recital 69)
Providers of on-demand AVMS “where practicable and by appropriate means”, promote the production of and access to European works. In particular, such promotion of European works takes the form of financial contributions services to the production of and acquisition of rights in European works, a minimum share of European works in the catalogues, or the attractive presentation of European works in electronic programme guides.

3.4.4. Rules applicable to linear audiovisual media services

3.4.4.1. Protection of minors (Art. 27)
Linear AVMS may not include any programmes which might seriously impair the physical, mental or moral development of minors, in particular those that involve gratuitous violence or
pornography. Other programmes which are likely to impair the physical, mental or moral development of minors can be shown on TV, but only on the condition that it is ensured, by selecting the time of the broadcast (known as the ‘watershed’) or by any technical measure (such as conditional access), that minors in the area of transmission will not normally hear or see such broadcasts.

3.4.4.2. European works (Art. 16)
Linear AVMS providers should reserve a majority of their transmission time (excluding the time allocated to news, sports events, games, advertising, teletext services and teleshopping) for ‘European works’.

3.4.4.3. Independent European producers (Art. 17)
Providers of linear media services should reserve at least 10 per cent of their transmission time (excluding the time allocated to news, sports events, games, advertising, teletext services and teleshopping) for European works created by producers who are independent of broadcasters. Alternatively, Member States may decide to impose a requirement that at least 10 per cent of a broadcaster’s programming budget be devoted to such works. The term ‘independent producer’ is not defined by the AVMS Directive and is thus left to the discretion of Member States.

3.4.4.4. Right of reply (Art. 28)
The AVMS Directive requires broadcasters to provide a right of reply to any natural or legal person whose legitimate interests, in particular reputation and good name, have been damaged by an assertion of incorrect facts made in a television programme. Alternatively, Member States can provide for equivalent remedies, which presumably would include broadcasting a full apology. Such remedies are without prejudice to any other remedies that may be available under or imposed by national law. The right of reply must exist in relation to all broadcasters under a Member State’s jurisdiction. Member States must adopt the measures needed to establish the right of reply or the equivalent remedies and determine the procedure to be followed for its exercise by an affected person. In particular, the procedures must allow the person concerned to exercise the right of reply (or equivalent remedies) appropriately, within a reasonable time of the request for a right of reply being substantiated and at an appropriate time and in an appropriate manner without imposing unreasonable terms or conditions. Member States must ensure that the right to reply (or equivalent remedy) is available to persons resident or established in other Member States. An application for a right of reply may be rejected if (i) it is not justified to protect the complainant’s legitimate interests (e.g. reputation and good name), (ii) would involve the broadcaster in committing a criminal offence, (iii) would render the broadcaster liable to civil law proceedings, or (iv) would transgress standards of public decency. Disputes as to the exercise of the right of reply must be subject to judicial review.

35 Art.17 AVMS Directive.
36 Art.28(1) AVMS Directive.
37 Art.28(2) AVMS Directive.
38 Art.28(1) AVMS Directive.
39 Art.28(3) AVMS Directive.
40 Art.28(4) AVMS Directive.
41 Art.28(5) AVMS Directive.
3.4.4.5. **Access to content: 'list of major events' mechanism (Art. 14)**

In short, the 'list of major events mechanism allows Member States to draw up a list with events, being of major importance for society, that can only be broadcast exclusively on a free-to-air television in order to ensure that a substantial proportion of the public would not be deprived of the possibility of following such events.

According to recital 53 of the AVMS Directive, free-to-air television refers to “broadcasting on a channel, either public or commercial, of programmes which are accessible to the public without payment in addition to the modes of funding of broadcasting that are widely prevailing in each Member State (such as licence fee and/or the basic tier subscription fee to a cable network)”. Since the definition is included in the recitals of the Directive, it is not guaranteed that free-to-air broadcasters will be of the same type in each Member State.\(^{42}\) Although it might be obvious that pay-television would not be labelled as free-to-air television due to the extra subscription fee and decoder purchase, the Danish Government, for example, considered (when the Danish list was still in force\(^ {43}\)) pay-television broadcasters charging fees lower than DKK 25 per month\(^ {44}\) as free-to-air broadcasters.\(^ {45}\)

Furthermore, it is required that “a substantial proportion of the public” would have the possibility of following the listed events. Given that the AVMS Directive does not contain a definition of the notion 'substantial proportion', it is up to the Member States to interpret this concept. In the U.K., for example, a free-to-air broadcaster wanting to broadcast listed events exclusively should be received by at least 95% of the households of the U.K.\(^ {46}\) In Austria, the listed events should be seen on a television channel accessible by at least 70% of the viewers.\(^ {47}\) In the Flemish Community “a large part of the population of the Flemish Community is considered to be able to follow an event of major importance to society on free-access television when the event […] and can be received by at least 90% of the population”.\(^ {48}\)

3.4.4.6. **Access to content: right to short news reporting (Art. 15)**

The right to short news reporting provision obliges all Member States to ensure the possibility for non-rights holding broadcasters to report about events of high interest to the public which are transmitted on an exclusive basis. These short extracts should not exceed 90 seconds.\(^ {49}\) A broadcaster should also be able to exercise this right through an intermediary acting specifically on its behalf on a case-by-case basis.\(^ {50}\) As a result, news agencies as such will not be entitled by Article 15.\(^ {51}\)

---


\(^ {43}\) In 2002, the Danish Government decided to revoke the Danish Order including the listed the events (Revocation of the Danish Order on the use of TV rights to events of major importance to society. *Of* (2002) C 45/7).

\(^ {44}\) DKK 25 is about 3.4 Euros.


\(^ {47}\) Art.2 of the Flemish Government establishing the list of events of major importance to society, Art.2.2 Order of the Flemish Government on the use of TV rights to events of major importance to society.\(^ {48}\) Art.2.2 Order of the Flemish Government establishing the list of events of major importance to society.

\(^ {49}\) Article 15 of the AVMS Directive; recital 55 of the AVMS Directive.

\(^ {50}\) Recital 55 of the AVMS Directive.

Member States should ensure that broadcasters can freely choose short extracts from the transmitting broadcaster’s signal or by other equivalent means, such as access to the venue of these events. As stated by Scheuer and Schoental, granting access to a recording of a programme and not to the signal of the event can not be considered to be an equivalent, because it “would not allow for an expedient use by the broadcaster exercising its right to short reporting and ensure a reasonable level of choice for, and quality of, the produced report”. Member States need to define the modalities and conditions regarding the provision of such short extracts: compensation arrangements, the maximum length of short extracts and time limits regarding their transmission. Such terms should be communicated in a timely manner before the event of high interest takes place to give other broadcasters sufficient time to exercise such a right. With regard to the compensation arrangements, the Austrian Bundeskommunikationssenat asked the Court of Justice to interpret Article 15 (6) of the AVMS Directive which foresees that “[…] Where compensation is provided for, it shall not exceed the additional costs directly incurred in providing access”. The question is whether Article 15 (6) of the AVMS Directive is compatible with the property rights of the broadcaster who bought the exclusive broadcasting rights and its freedom to conduct business, included in Articles 17 and 16 of the Charter of the Fundamental Rights of the European Union and Article 1 of the first protocol. This question arose in a dispute between the Austrian public broadcaster ORF and Sky Austria, being holder of exclusive broadcasting rights for a number of UEFA European League games. The Austrian broadcasting regulator had allowed ORF to use the Sky satellite signal for making short extracts for news programmes and decided that Sky could not ask for any compensation.

The country of origin principle applies to both the access to, and the transmission of, the short extracts. In a transfrontier case, this means that different laws should be applied sequentially. First, for access to the short extracts, the law of the Member State where the broadcaster supplying the initial signal (i.e. giving access) is established should apply (to determine the conditions for access to the short extracts). And then, for transmission of the short extracts, the law of the Member State where the broadcaster transmitting the short extracts is established applies (to determine the conditions for transmission of the short extracts).

52 Article 15 (3)-(4) of the AVMS Directive; recital 55 of the AVMS Directive.
54 Article 15 (6) of the AVMS Directive.
55 Recital 55 of the AVMS Directive.
60 The country of origin principle is the cornerstone of the AVMS Directive. According to this principle, media service providers are only subject to the national rules of one single Member State. All other Member States (receiving states) are prohibited from exercising a secondary control. For more information about the country of origin principle, see: P. Valck et al. (2010). The EU Regulatory Framework Applicable to Broadcasting. In L. Garzaniti & M. O’Regan (Eds.), Telecommunications, Broadcasting and the Internet. EU Competition Law & Regulation - 3rd ed. London: Thomson Sweet & Maxwell, 208-287.
61 Recital 55 of the AVMS Directive.
Schladming - Planai TV

Broadcasting rights for international sports events are often acquired jointly by all interested members, who then share the rights and the related fee between them. The FIS Alpine World Ski Championships will be held in Schladming in 2013. The broadcasting rights are jointly bought by the EBU and the Austrian public broadcaster, ORF, will broadcast the Championship. Planai TV, as a secondary broadcaster, has the right to short news reporting regarding this sports event. Planai TV should be able to freely choose short extracts from the transmitting broadcaster’s signal or by other equivalent means, such as access to the venue of these events. However, on the basis of mutual consultation, the parties concerned (the rights holding broadcaster and the secondary broadcasters) may deviate from the conditions included in these provisions. Hence, it could be possible that, after negotiations, ORF would allow Planai TV to use more than 90 seconds of the event. The right to short news reporting does only apply to events which are transmitted on an exclusive basis. If no exclusive broadcasting rights are sold, this provision does not apply.

3.5. Technology-neutrality

As already indicated earlier, the AVMS Directive is based on the principle of technological neutrality. This implies that all providers of audiovisual media services, irrespective of the platform or technology used to deliver the services. Hence, rules on cultural diversity, protection of minors and human dignity, commercial communications, etc., not only apply to traditional, linear broadcasters, but also to providers of on-demand media services. There are, however, two important limitations to the implementation of technological neutrality in the directive.

Firstly, on-demand services are subject to lighter rules than linear services, because of their perceived lower impact on society and the larger control of the user over the selection and moment of viewing (supra).

Secondly, the scope of the directive is confined to audiovisual media and does not cover text-based media (supra), which have traditionally been subject to self-regulation only. Broadcasting and publishing are still seen as two distinct activities (linked to fundamentally diverging regulatory frameworks), despite the growing convergence between both. Today, online news services are a mix of video clips with textual commentaries, digital TV channels offer programmes enriched with additional information that combines text and video, or provide viewers the opportunity to chat on the screen while watching. Large media companies are active both in print and audiovisual media, and re-use content produced for one outlet (e.g. newspaper) on other platforms (radio, TV, internet). It is a reality that on-demand services, both on websites of newspapers and broadcasters, represent an increasingly important part of the audiovisual media market. However, given that recital 28 AVMS Directive explicitly excludes electronic versions of newspapers and magazines from the scope of this Directive, on-demand services on newspapers’ website do not have to comply with the same strict rules as on-demand services on broadcasters’ website. For example, while broadcasters have to comply with strict sector-specific

---


© Copyright KU Leuven and other members of the EXPERIMEDIA consortium 2012
rules for advertising, sponsorship, product placement, etc., journals and magazines only have to comply with general advertising rules (e.g. in unfair commercial practices acts) and ethical codes. The last decade, we can witness an increasing technological and economic convergence between text-based media, on the one hand, and audiovisual media, on the other hand. Newspapers are increasingly offering audiovisual material alongside their ‘normal’ articles and broadcasters themselves increasingly invest in text on their dominantly image-driven websites. Given that it is not always clear which rules apply to these grey-zone services, it comes as no surprise that uncertainty and distrust is created in the media sector. The question that rises is whether there is a difference between on-demand services of an online version of a newspaper and on a broadcaster’s website and whether it justified that other rules apply to similar services.
4. Copyright

4.1. Introduction
As already indicated above, due to technological evolutions, the public is now afforded the opportunity to produce its own (sports) content and distribute it on the Internet. One of the most commonly expressed concerns about audiovisual content, and in particular UGC, refers to Intellectual Property Rights: how can the public produce and create its own content without a danger of infringing rights of authors. The broad range of content created by the Internet users (video, photographs, text, music, games, etc.) complicates the whole matter as sometimes different rules may apply. For this reason the following chapter provides an explanation of the most important concepts of this area of law.

4.2. No harmonization
Works such as films and television programmes are protected under national law by copyright or neighbouring rights (such as fixation, reproduction and distribution rights). Differences in the legal protection provided by the laws of the Member States for copyright works created barriers to trade and distorted competition and thereby impeded the creation and functioning of an internal market in broadcasting services. As a result, legislation has been adopted at the EU level to harmonise national laws on copyright and related rights, for example with regard to the term of protection.\(^{63}\) In 2001, the Information Society Copyright Directive\(^{64}\) was adopted to introduce a series of harmonised provisions applicable to all fields of the Information Society. However, other relevant EU legislation remains relevant to particular segments of the Information Society, including: rental, lending and resale rights; the copyright protection of databases, computer programmes and semiconductor topographies; and the copyright protection of programmes broadcast by satellite and cable retransmission. In addition a directive on the enforcement of intellectual and industrial property rights such as copyright and related rights, trademarks, designs or patents was adopted in 2004.\(^{65}\)

Despite the different Directives, it should be clarified that copyright law in Europe is not fully harmonized. This means that there are many differences between countries in the European Union in how they regulate these issues. On the very general level, the concepts of a protection of intellectual creation are understood in a similar way, however specific laws of countries vary in this respect. Such situation refers for example to a major criterion in copyright which requires a creation to be ‘original’ in order to receive protection. At the European level, only three categories of works, specifically computer programs, photographs, and databases enjoy a harmonized requirement of originality.\(^{66}\) These three types of works must constitute the 'author's

---


own intellectual creation' to receive legal protection. The criterion of originality for all the other types of works is determined at the national level. This is often considered as a grand difficulty as the minimum amount of creative effort necessary to give rise to copyright protection depends on the context, and on the national copyright law of the Member State. The levels of originality range from the rather low requirement of ‘skill and labour’ in the UK, through the medium requirement of ‘the individual character and the personal stamp of the author' in France and Belgium, to a demanding requirement of the 'print of the author's personality that rises above average' in Germany.

The described situation leads to two conclusions. First, not all content is protected by the copyright law. Only the content which fulfils the necessary criteria of a particular country falls under the protective shield of the law. Second, it is possible that some content can be under protection in one (or several) Member States but not in another. This is a result of the different level of originality applied by the countries. Moreover, in both cases the final decision is always left to a court which is the only competent body to conduct an interpretation of a legal provision. After this is done the rule is measured against a specific case and only then the court can provide the final answer and decide whether a particular piece of work falls under copyright protection. This means that there rarely are clear situations and most of the time an element of ambiguity occurs. A necessary analysis is always done on a case-to-case basis. In some situation it might be clearer than in others but unless there is a court’s decision the assessment is never definite. This however does not mean that all the cases are analysed by the courts. This happens solely if one of the parties, like the author, feels that his rights have been violated.

**FHW – 3D movie**

A very wide range of works are copyright protected if the necessary criteria are fulfilled. A creation needs to be original in order to receive protection. The 3D movies shown in the Tholos will probably be copyright protected because this work could be regarded as original.

**Schladming – User-generated video streaming and sharing**

The UGC that will be uploaded on the YouTube like or Facebook like services of Schladming could be copyright protected if it could be labelled as original. However, it is important that one realizes that they are infringing intellectual property rights when they are using specific content (*infra*).

---


© Copyright KU Leuven and other members of the EXPERIMEDIA consortium 2012
4.3. **Public domain**

Another concept that requires explanation is ‘Public Domain’. This notion is often wrongly understood as describing the accessibility of a creation. This might be especially confusing with regard to the content available on Social Networks. If a text or a photograph is publically visible on an open profile or account it is often referred to as being in Public Domain and freely available for re-use. This however is not correct. Public Domain is defined as “all the knowledge and information – including books, pictures and audiovisual works – which does not have copyright protection and can be used without restriction”. It contains two types of materials, works on which copyrights has expired (general IPR in most of Europe is 70 years after the death of the author) and materials that has never been covered by copyright. In the case of the latter it means materials that are not original enough to receive protection. This, however, has nothing to do with the work being openly presented on Social Networks or any other platform. It should be noted that the presentation of a creation to a broad public does not cease the existence of a copyright protection. The fact that the author decided to present his work to the online audience in no way deprives him of the rights that he obtained with the moment of finalizing his creation. There is no requirement of an acceptance or declaration of existence of copyright. No certification of an official body is necessary to initiate protection. Even the commonly recognized symbol © is not required in Europe to mark the protected works. This is an additional difficulty as anybody interested in re-using a work needs to put a lot of effort in to find out who the right owner is and to check the correct copyright status of a work.

4.4. **Copyright holder**

To sum up the relevant information so far, once a suitable content is found, a question about its protection must be answered. If the content is original it is most likely protected by copyright law. Next, a copyright holder has to be identified. In the case of the UGC most of the times it will be the author of the work, but this is not necessarily the case, for example if the (exploitation) rights have been assigned to a third party. The owner of the copyright is the sole actor to whose discretion an authorisation or a prohibition of certain uses of the work is left to.

4.5. **Exceptions**

Account should also be taken of possible exceptions and limitations on copyrights. Such exceptions define when in a legitimate interest of the users certain unauthorized uses of the copyrighted material are allowed. The exceptions that are most commonly present in copyright legislations relate to private copying, quotations, parody, public speeches, news reporting and the limitations to the benefit of educational institutions, libraries, and disabled persons. The problem is that the lists of exceptions vary from country to country. There exist one common list of exceptions in the Directive 2001/29/EC, but each Member State is free to choose which exceptions it is willing to implement into the national law (cherry picking). This makes potential use of copyrighted material difficult as one exception that would allow to use the material without a need to worry about infringing the author’s rights might be present in one country but not in another.

---

4.6. Terms of Use

Apart from the general rules presented above also conditions described in Terms of Use (or Terms of Service) of any platform with UGC might influence the possibility of re-using the content of these platforms. Such Terms of Use constitute a contractual agreement between a service provider and a user. Acceptance of the conditions of Terms of Use, usually together with Privacy Policies, is required for the provision of the service. Conditions contained there define a relationship between the service provider and the users and describe the rights and obligations of the involved parties. ToU regulate a broad range of issues like e.g. liability, applicable law or Intellectual Property Rights and allowed use of the platform’s content. The approach towards this last matter varies dramatically from platform to platform. This is mainly a result of a general concept of a specific platform and its main purpose. In case of Twitter re-use of the platform’s content is endorsed/encouraged as the ToU explain that “We encourage and permit broad re-use of Content”70. The problem of IPR is dealt with through a condition according to which users grant the platform and other users “a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed)”. A possible re-use of the content by third parties is addressed very extensively. It is also clarified in simple terms that the user retains his rights to any content he submits, posts or displays on or through the Services.71 Facebook, on the other hand, limits itself to a short statement that any content posted on a publically open profile can be re-used by others.72 Such an approach could be explained by the fact that the primary purpose of this Social Network is communication with friends and any Twitter-like activities are rather a by-product of this platform. With reference to content protected by copyright, like photos or videos, users grant Facebook “a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License")”. As there is no common stand across the existing platforms a case-to-case analysis is advisable. In case a platform’s policy in this regard is unclear it is recommended to obtain consent from the content creator directly. This way any legal uncertainty in this matter would be solved.

In conclusion it should be said that the issues stemming from the Intellectual Property Rights with regard to the UGC are rather complicated. The main reason for this is a lack of harmonization of the subject matter across Europe.

4.7. Copyright and sports events

4.7.1. Sports events: copyright protected or not?

There is discussion in literature whether sports events could be copyright protected or not. The major part of the authors indicate that sports events as such are not protected by copyright (attributed to authors) or related rights (attributed to performers, producers and broadcasters). A sports event is nothing but a mere fact, pure information falling outside the scope of copyright as it does not fulfil the two basic conditions needed to acquire copyright protection, namely ‘originality’ and a ‘concrete character’. It is exactly the first characteristic that a sports event, like

for example a football game, lacks. Consequently, neither the athlete nor his sports team can create a monopoly on his sporting achievements through the use of exclusive rights to protect his or economic (leave alone moral) interests.\textsuperscript{73} In the Premier League case\textsuperscript{74}, the Court of Justice explicitly stated that the “FAPL cannot claim copyright in the Premier League matches themselves, as they cannot be classified as works”.\textsuperscript{75} Furthermore, the Court of Justice indicated that “sporting events cannot be regarded as intellectual creations classifiable as works within the meaning of the Copyright Directive”. This reasoning applies in particular to football matches, which are subject to rules of the game, leaving no room for creative freedom for the purposes of copyright.\textsuperscript{76} Although sports events are not protected by under copyright, the Court stressed that sporting events, as such, have a unique and, to that extent, original character which can transform them into subject-matter that is worthy of protection comparable to the protection of works, and that protection can be granted, where appropriate, by the various domestic legal orders.\textsuperscript{77} Accordingly, it is permissible for a Member State to protect sporting events, where appropriate by virtue of protection of intellectual property, by putting in place specific national legislation, or by recognising, in compliance with European Union law, protection conferred upon those events by agreements concluded between the persons having the right to make the audiovisual content of the events available to the public and the persons who wish to broadcast that content to the public of their choice.\textsuperscript{78}

Still, it is not always easy to draw the line between what is copyrightable and what is not. It would be reasonable to state that the main difference lays in the fact that — contrary to, for example, a theatre play — sports people do not follow an underlying script, but are rather subject to unanticipated occurrences.\textsuperscript{79} Yet one might wonder why, for example an ‘artistic performance’ such as a dance performance, a concert or a theatre play is protected by copyright and related rights (attributed to performers dancers, singers, actors, musicians), whereas a performance by an athlete in for example, artistic gymnastics, synchronized swimming or figure skating, does not. This distinction could be rather questionable.\textsuperscript{80} The different treatment could be explained by the “competition aspect” of sport. Even where athletic preparation most resembles authorship, a performer who conceives and executes an acrobatic feat can not copyright it without underlying competition in future.\textsuperscript{81} However, some authors indicate that sports events will not qualify for copyright protection, except sports involving a choreographed script (such as synchronized swimming or figure skating).\textsuperscript{82} In other words, when sports moves are reduced to writing, they become a protected work.
It is questionable whether the routines of synchronised swimming will be copyright protected. However, choreography of synchronised swimming could not be compared to a football game. A football game lacks any originality, while a choreography of synchronised swimming requires a certain level of originality in order to arrange the movements in a specific sequence.

4.8. UGC and sports events

The new media technologies have offered the public (including the athletes themselves) the opportunity to produce their own audiovisual content or run their personal blogs to report and express their personal opinion on sports events. In other words, citizens now have a place next to traditional producers of sports content in the digital sports landscape. Given that games and sports movements are not protected by copyrights, anyone inside the stadium is therefore allowed to record the game (from a copyright point of view). However, as the saying goes, ‘all that glitters is not gold’. The Internet does not only provide the citizens to distribute original content, it is also swarming with illegal content that infringes the rights of others. In particular, sports events, being covered by exclusive media licensing agreements, are now on a large scale copied by fans without the authorisation of the rights holders involved.

Sports events are usually brought in a format leading to legal protection. Once the sports event has been broadcast, for example, the broadcast itself is protected by copyright as an audiovisual work, and by related rights attributed to the producer who invested in the (first) fixation of the broadcast. As a consequence, the reproduction, communication to the public and further distribution of that broadcast, news coverage or film requires the authorisation (license) of the right holder. In practice, this will always be a broadcaster. Broadcasters and sports organisations have put up fights to protect rights. The Premier League, for example, decided to sue YouTube, for posting user-generated videos that infringe copyrights and exclusive deals with other media operators. Both Viacom and the Premier League lost the case in first instance. According to the US Court, YouTube is not infringing copyright when the public is posting unauthorised videos to the site. YouTube only becomes liable for infringement when it does not immediately remove videos from its website once it has been told that these videos infringe specific copyrights. During the Beijing Games in 2008, the International Olympic Committee (IOC) requested the Swedish authorities for the removal of copyrighted Olympics content illegally stored on the peer-to-peer network PirateBay.

Furthermore, there is a recent trend towards prohibiting users from producing content. However, terms and conditions of different football teams and sports organisations contain the

85 E. Werkers et al. (2008). One world one dream? Sports blogging at the Beijing Olympic Games. ISLJ, 45.
86 Ibid., 45.
prohibition for ticket holders to “bring into (or use within) the Ground any equipment which is capable of recording or transmitting (by digital or other means) any audio, visual or audio-visual material or any information or data in relation to a Match”.89 Furthermore, in June 2011, The Times obtained information that Apple wants to stop iPhone users from filming live events, such as sports events or concerts, with their smartphone. According to The Times, Apple is developing software that will sense when a smartphone user is trying to record a live event. Sensors would automatically instruct the iPhone to shut down its camera function. Other features, such as texting and making calls, would still work.90 According to The Times, the development of this software is seen as an attempt to protect the exclusive rights holders.91 Hence, these prohibitions and restrictions limit the fans’ and sports clubs’ possibilities to upload audiovisual material of matches on the Internet. Or in other words, it limits their ability to become legitimate providers of online sports content.92

However, some sports organisations have embraced the opportunities created by user-generated content. They realised that user-generated content could create opportunities apart from threats. Some sports organisations have agreed a deal with YouTube to share their sports content.93 During the 2006 FIFA World Cup, for example, one of the new media innovations was the involvement of the public in user-generated content, which included participation and involvement through self-production of videos and pictures.94 Furthermore, Santomier & Costabiei argued that, from a content distribution perspective, sports organisations should develop a strategy for integrating appropriately selected user-generated content with traditional sports content. In particular, sports organisations will determine which content will be made available via digital feeds to the public offering the latter the possibility to create their own services, such as a video or a blog.95

However, the fact that sports broadcasting rights sold in an exclusive way should not deny citizens from shooting videos of the atmosphere.

### Schladming - User-generated video streaming and sharing

The content created and uploaded by the public could be copyright protected. However, it is important that the public realises that they are infringing intellectual property rights when they are using specific content. Furthermore, visitors of the FIS Alpine World Ski
Championships in Schladming in 2013 should realize that the public broadcaster owns the exclusive broadcasting rights which could limit them in recording the sports event and uploading videos on a social network site. However, they are not denied from shooting videos of the atmosphere.

4.9. Open content licenses – Creative Commons

Copyright is often imposing legal and policy barriers to the sharing and re-using of (user-generated) content. However, a number of access and licensing policies that remove and minimise these barriers have been developed. In this deliverable, creative commons licences will be described.

4.9.1. Introduction

Open content licenses are an externalization of the U.S. 'Free Culture' philosophy. The rationale of the 'Free Culture' philosophy is simple: original -and thus copyright protected works- should be made freely available on the Internet by means of a variety of flexible licenses, being the so-called 'open source licenses' and 'open content licenses'.

The first open source license initiative was taken in the field of software. Some software developers opposing the monopolies in the software market started using open standards and encouraged the use of 'open source software' or 'free software'. These developers allowed under certain conditions that users saved, used, copied and adapted this open source software to their own needs. Furthermore, the users of the free software could redistribute the new software that resulted from their adjustments and edits. However, in such a case, the original developer often demanded that further distribution of new software based on his original source code could only occur under the same licensing conditions as the original source code and if the original source code was specifically mentioned when distributing the new software. In this case we speak of a so-called 'copyleft license'. This 'copyleft' system was integrated in among others the 'GNU General Public License (GPL), one of the most advanced open source licenses'. It should however be noted that such a license in no way implies a waiver of all copyright. The goal of this license is simply to make sharing and re-using of software code more efficient, by eliminating a priori some hampering effects of copyright protection on this type of works. Proponents of this type of software refer to advantages such as increased choice for users, better interoperability, accelerated development of new technology, decreased development cost, etc.

---

96 Not to be confused with 'shareware' (a software program can be tested for a certain period by a user, if he wants to continue the use after the testing period, he has to start paying a license fee) or "freeware" (a software program can be used for free and be distributed as well). The word 'free' in 'free software' refers to the freedom of use (what can be done with the software), not the fact whether or not the use is 'for free' (no payment).


The creation and proliferation of open licenses did not remain limited to the software sector. Also with regard to cultural content a demand for more flexible copyright licenses that allowed a more efficient dissemination of works among the public grew. This demand was mostly driven by the opportunities offered by an ever expanding internet, offering ever increasing interactivity. With the idea to spread ‘open / free content’ online in order to improve creativity and innovation, the best-known open content licenses came to life: the "Creative Commons" licenses.

4.9.2. Creative Common (CC) Licenses

The CC initiative was set up in 2001 by a group of academics specialized in internet and intellectual property law, computer science and new media. The first set of CC licences was released in 2002 and in 2008 almost 50 national translations are available, adapted to national law and terminology.

CC licenses try to realize for other copyright protected subject matter, what the ‘GNU General Public License made possible for software. The CC concept is based on the idea that not all rights, but ‘some rights reserved’ is sufficient to protect the authors of copyrighted works. Copyright should be exercised in a way that the author is still protected but the sharing and use of the works is encouraged at the same time. CC licenses are in fact intended for any possible copyright protected work (music, photos, video ...) and can therefore be used by all kinds of authors (musicians, photographers, filmmakers, writers ...). It is important to emphasize that CC licenses do not imply a complete waiver of copyright by the author. The widespread use of CC licenses would definitely not result in an internet as parallel legal reality in which copyright has no meaning. CC respects the existing legal framework concerning copyright and its system of automatic allocation of an exclusive right for the author. CC also respects the legally correct way to transfer or release copyrights from one person to another. In this sense, authors do nothing more than offering a broad license for which no copyright fee must be paid in return, yet they also retain certain rights.

One of the most typical features of the CC licenses is the fact that the copyright holder does not conclude this agreement with one specific contractual counterparty, but in principle a priori with any potential third party. Everybody who is interested in using the work may within the limits of the specific license attached to it is allowed to do so, without contacting the right holder. Another core feature of the CC are the simplicity of its standardized terms, instant authorization to any member of the public who wants to use the work, and increased potential for broad distribution of the work. Simplicity is needed, because without it widespread acceptance will be difficult.

---

The CC licenses have been translated into and adapted to different national legislations resulting in a cross-border application of these licenses (which makes them perfect for online uses of protected works) and their specific symbols (which improves usability and branding on a global scale).

The CC licenses include the right to copy the work, distribute it, display it or perform it publicly. If the material is publicly distributed, displayed or performed, a copy of the CC licence must be included. The licences allow world-wide use on a non-exclusive basis and they are irrevocable. This means that once an author has chosen to make material available under a CC licence, he cannot go back and withdraw the permissions so granted. Hence, the user is sure that he can continue to use the work and e.g. make and licence derivative products. The licence ends only if the licensor acts in breach of the licence terms and conditions. In addition, to ensure that users retain access to the material under the terms that were originally determined by the rights holder, no user is allowed to use technological measures to restrict other users’ lawful use of the work.

The material is offered ‘as is’, without any warranties and with a disclaimer of all liability. The licences are granted royalty-free, so they do not provide for any remuneration for the use of the material. As Van Eechoud and Vanderwal clarify, “licensing a work under CC does not prevent the licensor from charging recipients for the distribution of copies, for instance to cover the costs of a medium. The royalty-free clause prohibits costs for content, but not for packaging”. However, as much of the material that is the subject of CC licences is made available via the internet, the costs of distribution will be non-existent. Next to charging for the packaging, the rights holder can also make money from the material itself, if he chooses the right licence. If he uses the CC licence under which no commercial use is allowed, he will still be able to charge for commercial use under a different licence, or request payment separately on the website.

The licence can be drafted in an automated process on the CC website. Once the rights holder has made a choice between the six types of licences (infra), the licence is created in three formats. First, there is the actual legal licence, which determines the rights and obligations and will be the subject of any court dispute. Second, this licence is translated into ‘human readable language’, explaining the main terms and conditions of the licence in everyday language and with standard symbols. Finally, the licence is also created in a machine-readable format, making it possible for the licensing process to be automated and for search engines to include searches on CC

---


material. While the licences are particularly intended for the dissemination of material on the internet, they can also be used for other media.

There are different types of CC licenses, each with its own label, granting users more extensive or more limited rights with respect to the work to which the license has been attached. The CC system allows the authors to make a tailor-made license, expressing exactly to which extent he wishes to accept free (re-)use of his work. In other words, CC gives an author or rights holder the choice between a number of different licences that vary from open to more restrictive, depending on the conditions that are included. The author can choose whether the work can be modified by the user or it can only be used verbatim, whether the work can be used for commercial purposes or not, and whether the user should grant the same rights when he creates a derivate work and makes this available to the public.

CC offers six standard licenses, each with its own specific characteristics and each granting users a different level of rights. Each of the six licenses requires that the name of the (original) author is mentioned when the work is being used in order to respect the author's legal paternity. This is called ‘Attribution’. Apart from this minimum requirement, the author who wishes to link a CC license to his work should make a number of trade-offs. Could a licensee use the work for commercial purposes? Can the licensee adapt the work? Should the licensee offer his adapted work (a derivative work or a compilation) under the same license to others or not? (they are speaking also about 'share alike' or 'copyleft')?

The combination of these conditions leads to six types of licences. CC created specific symbols for different variables within the license.

The Attribution Licence


109 We can not give an extensive description of all the different issues related to the different CC licenses. A lot of very well-structured information can be found on the CC website www.creativecommons.org.
This CC license offers rights to the user in the broadest sense. It allows users to edit the work, reproduce it and reuse it in new works and publicly communicate it, for commercial purposes. Derivative works based on this work can also be distributed under a different license than the initial "Creative Commons" license. The user must mention the rights holder’s name.

The Attribution Share Alike Licence

This license grants identical right to user as the previous ‘Attribution license’. However, derivative works can only be made available to the public under the same ‘Attribution – Share Alike’ license. Consequently, all derivative authors have to allow that their work can be used in a (non-)commercial context. The user must mention the rights holder’s name.

The Attribution No Derivative Works Licence

This license implies that a third party can reproduce and distribute the work, both in a commercial and a non-commercial context, yet without modifying the work partially or as a whole. He can use the work as it is. The user must mention the rights holder’s name.

The Attribution Non-commercial Licence

Under this license, users are allowed to edit the work (i.e. translate, remix, improve, etc.) and communicate it to a public, but only when there is no commercial purpose involved. On the other hand, the derivative work based on the original work can be distributed with another type of license, even a license that allows for commercial use of the derivative work (not the original!). The user must mention the rights holder’s name.

The Attribution Non-Commercial Share Alike Licence

This license grants identical rights to users as the ‘Attribution – NonCommercial’ license. However, derivative works can only be made available to the public under the same ‘Attribution – NonCommercial – ShareAlike’ license. Consequently, all derivative authors have to forbid that their work can be used in a commercial context. The user must mention the rights holder’s name.

The Attribution Non-commercial No Derivative Works Licence
This license allows that the work is being downloaded and shared with others, provided that it is not altered in any way and that it is only used for non-commercial purposes. The user must mention the rights holder’s name.

**Schladming - User-generated video streaming and sharing**

In order to ensure that the user-generated content of the visitors of Schladming can be used by other visitors by Schladming 2030, users can be asked to attach the Attribution Share Alike Licence to their uploaded content. Everybody who is interested in using the work may within the limits of this specific license is allowed to do so, without contacting the rights holder.
5. Privacy policy framework

5.1. Introduction

One of the legal risks associated with EXPERIMEDIA is how to comply with current and future privacy regulations. As privacy is becoming more of a genuine concern to the citizen and as threats to the citizen’s privacy are becoming more pervasive, it becomes clear that providing a satisfactory level of privacy protection will be one of the most pressing issues to be resolved before expecting the citizen to put his trust into the different experiments. Therefore, this chapter aims to provide a coherent view of the current legal framework regarding privacy protection, with specific attention to the main privacy concerns relating to the experiments.

First, an overview will be provided of the current legal framework regarding privacy protection in the EU. More in detail, the main focus of this sector will lie on the EU framework regarding data protection found in Directive 95/46/EC.110 Given the nature of a directive and its need for national implementation by the EU Member States, a concise overview will be provided on the major differences in the national implementations of this directive by the Member States. As Directive 95/46/EC is currently impending review, this chapter will also look forward to the expected changes. Second, this chapter will take a closer look at some of the more specific privacy concerns. Some of these issues – such as the line between the notions of controller and processor, the limits of the concept of personal data, the implementation of the principle of proportionality – focus on the limitations of the definitions currently employed in the EU legal framework on data protection, while other issues focus more on the interaction with the data subject – such as how to obtain the data subject’s consent.

5.2. General privacy regulation

From the following overview of legal instruments regarding this matter, it becomes apparent that privacy regulations have only become widespread and commonly accepted since the second half of the 20th century. The right to privacy therefore is a relatively young notion, although one may argue that the need for privacy even predates humanity. Within Europe, the right to privacy can mainly be found in article 8 of the European Convention on Human Rights (ECHR).111 This article concerns the private and family life, home and correspondence of the citizen. Although this article is still one of the foundations of European privacy protection, its value in the field of data privacy has been surpassed by the more enforceable instruments of the EU. Apart from Directive 95/46/EC, the EU has also provided for privacy protection in the field of electronic communications (Directive 2002/58/EC112) and in the field of data retention (Directive 2006/24/EC113). Furthermore, the EU has included the right to privacy, as well as the right to

---

111 Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome, 4 November 1950. Note that this is an instrument of the Council of Europe, not of the EU.
data protection, in the Charter of Fundamental Rights of the European Union\textsuperscript{114}, anchoring the value of human rights protection in the Treaty on the European Union\textsuperscript{115}.

5.2.1. Directive 95/46/EC

The idea of data privacy gained foothold in Europe after the Organization for Economic Co-operation and Development (OECD) published guidelines on the protection of privacy and transborder data flows.\textsuperscript{116} These guidelines served as the inspiration for the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.\textsuperscript{117} Given the lack of support for this convention, yet realizing the need for adequate data protection across Member States, the EU started work on a directive on the matter in the early 1990’s using the basic principles laid out in the aforementioned Council of Europe Convention. Finally, on the 24 October 1995, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (commonly known as the Data Protection Directive) was accepted. Implementation into national legislation by the Member States was expected by late 1998. Note that Directive 95/46/EC aims to protect only the fundamental rights and freedoms of natural persons\textsuperscript{118}, although some Member States have decided to expand its scope of application, offering protection to legal persons as well.

5.2.1.1. Definitions and scope

Article 2 of Directive 95/46/EC states a number of definitions, delineating the precise scope of the directive. More specifically, the directive provides definitions for the notions of personal data, processing of personal data, personal data filing system, controller, processor, third party, recipient and the data subject’s consent.

**Personal data**

*Introduction*

The core of Directive 95/46/EC is the notion of personal data. This is defined as:

\[
\text{…any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.}
\]

Note that the directive does not distinguish between written, oral, visual or any other type of information. Furthermore, the information needs to identify a natural person or make this person identifiable. A person can be considered as being identified when his identity can directly be established. This is the case when using a national single identification number of general application.\textsuperscript{119} As such an identification number is uniquely assigned to every single citizen, this

\textsuperscript{114} OJ. C 83 of 30 March 2010, 393.
\textsuperscript{115} Ibid., 19.
\textsuperscript{116} OECD Recommendation of the Council of 23 September 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data.
\textsuperscript{117} Convention nr. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed at Strasbourg on 28 January 1981.
\textsuperscript{118} Article 1 Directive 95/46/EC.
\textsuperscript{119} A national single identification number of general application is an identification number attributed by States to their citizens in order to uniquely identify them. Such identification numbers are used in, for instance, Belgium, Sweden and Spain.
citizen can be directly identified using this identification number. Other examples include name, address, date of birth, etc. While these last examples are not necessarily unique for one single citizen, they carry a high probability of direct identification of the person involved. If the person involved cannot be identified directly, he may still be identified indirectly by combining different elements or by deducing other identifiers from available information. In such case, the person is identifiable. This definition leads to a very broad spectrum of information that could potentially serve as personal data.

**Limits of the concept personal data**

As the definition of the concept of personal data in the directive has a very broad scope, its precise interpretation appears to differ amongst Member States (*infra*). Aiming to provide a more coherent interpretation across the EU, the Article 29 Working Party adopted an opinion on the concept of personal data. As this concept forms the very basis of the EU legal framework on data protection, a coherent and homogenous interpretation by all Member States is of utmost importance. Although it could be argued that the definition of the concept of personal data has deliberately been formulated in a broad manner in order to embed flexibility in the application of the concept to various circumstances, it should also be noted that the scope of the concept should not be overstretched. Here, the Working Party clearly states that it would be undesirable to stretch the existing concept for application to situations not intended to be covered by the legislator, which is an appropriate reaction as the idea of overstretching the applicability of existing concepts is one of the core issues that augmented the demand for review of the directive. However, the Working Party also warns for a too narrow application of the directive. When the application of the concept of personal data may at first sight seem to be overstretched, one should first look at the scope of the directive, in particular article 3. Next, one should look at exemptions or simplifications in the directive or in national implementations thereof. The Working Party addresses the national Data Protection Supervisory Authorities (DPA) to monitor the application and interpreting of the directive and to endorse a broad definition of concepts for application of the directive to societal and technological evolutions.

The Working Party continues its opinions by analysing the constitutive elements of the concept of personal data. First, the element of information is analysed. Here, it is indicated that nature and content of the information are of no importance as all information is included under the scope of the directive, regardless of nature or content. From this, one can deduce that the directive is not limited to the protection of information regarding the strict sphere of home and family, but also touches subjects beyond this sphere such as labour law, court records and direct marketing. Also the format or medium used in presenting the data is of no importance.

---

121 Ibid.
122 Ibid.
124 Article 8 (2) (b) Directive 95/46/EC.
125 Article 8 (5) Directive 95/46/EC.
126 Article 14 (b) Directive 95/46/EC.
Second, the information needs to relate to an individual.\textsuperscript{127} This can be a direct relation, where information about a person is given.\textsuperscript{128} Also possible is an indirect relation, whereby information is provided on an object that relates to the individual.\textsuperscript{129} In short, the Working Party considers data to relate to an individual if “it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated”.\textsuperscript{130} According to the Working party, information can relate to an individual if there is a content element\textsuperscript{131}, a purpose element\textsuperscript{132} or a result element\textsuperscript{133}.

Third, regarding the element of identified or identifiable individuals,\textsuperscript{134} the Working Party notes that this means that the individual should be distinguished from the other members of the group, or that it should be possible to do so. Directly or indirectly refers to the degree of precision by which a certain identifier can indicate a single individual.\textsuperscript{135} For indirect identification, one will have to combine several elements of information together before a unique identification can be made. For defining the notion of identifiable, the Working Party refer to recital 26 of the Directive where identifiable is defined as all the means likely reasonably to be used to identify an individual. By determining what is likely reasonably to be used one, has to keep in mind several factors – such as the cost of identification – and reality has to be applied. Hypothetical possibilities for identification are not likely reasonably to be used and are therefore not to be considered as personal data. The Working Party also makes note of the use of pseudonymisation of data to disguise identities and of anonymisation to make identification impossible.

The last element analysed by the Working Party is that of the natural person.\textsuperscript{136} As explained earlier, the directive protects the rights and freedoms of natural persons. In this opinion, the Working Party elaborates on the fact that this data is generally regarded to relate to living natural persons. Therefore, two particular cases could come to mind: the dead and the unborn.

In general, the dead are no longer regarded as being part of the concept of natural persons and are therefore excluded from data protection rights. Exceptions to this rule may, however, apply. For one, if the controller is not certain of a person’s death, he will process data relating to that person as if he were living. Data relating to the dead may also provide information on the living, for instance hereditary medical conditions, and is therefore to be processed according to the applicable provisions in the directive. Regarding medical data it should also be noted that confidentiality duties continue even after death.

Although most, if not all, Member States have reached consensus on the end of life, there are still differences in national legal systems on the beginning of life, complicating the case of personal data relating to the unborn. One will have to look into the national provisions on rights


\textsuperscript{128} The Working Party lists medical and personnel records as examples of files in which data relating to an individual can be found.

\textsuperscript{129} The value of a house can, for instance, give information on the assets and wealth of its owner.


\textsuperscript{131} If information on an individual is given, regardless of any specific purpose.

\textsuperscript{132} When data is provided for a specific use.

\textsuperscript{133} When the data provided can have an impact on an individual’s rights and interests.


\textsuperscript{135} This is obviously a contextual matter. The notion “man in business suit” may not provide much help for identifying a particular individual on Wall Street, while it may be useful to single out someone in a more rural crowd.

relating to the unborn in order to establish whether a particular State grants data protection rights to this case.

Note that, if certain data appears not to be personal data under the scope of the directive, one might have to look at national implementation thereof as these may have enlarged the scope of the directive. The pending review of the directive may also have implications to the precise scope of the concept of personal data.

With these analyses of the core notions of the concept of personal data, the Article 29 Working Party hopes to have cleared the precise scope of this foundation of the EU legal framework on data protection.

**Schladming – Personal data**

The provision of innovative future internet technology solutions to the visitors and citizens of Schladming is largely based on the processing of information that relates to them either directly or indirectly. Therefore the processing of such information should be carried out in accordance to the provisions of the Data Protection Directive.

**FHW – Audience interaction**

The interaction of the audience with the experts and with the equipment of FHW reveals information about the choices of users, which may relate to them. In such cases the relevant information should be considered as personal data and be processed in compliance with the Data Protection Directive.

**Processing**

Second, the personal data needs to be the subject of processing of personal data. Processing is defined as:

> …any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Also in this case, Directive 95/46/EC gives a very broad definition of this notion. Virtually every act in which personal data is used can be considered as a form of processing. Note that both automatic and non-automatic processing can fall under the scope of this directive.

Regarding the precise scope of the directive, article 3 states that the directive is not applicable to processing:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the
economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

The second exception – often referred to as the household exception – is not clearly defined in the directive.

Article 9 provides an exception for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. More exemptions for public authorities are provided under article 13.\(^{137}\)

**Personal data filing system**

A personal data filing system is:

…any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Note that unstructured data is excluded from this definition.\(^{138}\) Furthermore, the data needs to be accessible according to certain criteria. According to recital 27 the structure needs to relate to such criteria.

**Controller and processor**

**Introduction**

The main actors performing the processing of personal data are the controller and the processor.

The entity responsible for the processing is the controller. This is:

…the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

The main criterion in this definition is the authority to determine the purposes and means of the processing.\(^ {139}\) Note that, while the directive is only aimed at protecting the fundamental rights and freedoms of natural persons, the controller can be both a natural person and a (public) legal person. Joint responsibility in case of multiple entities collaborating is also an option.

---

\(^{137}\) Obligations and rights may be restricted for safeguarding: “(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (e), (d) and (c); (g) the protection of the data subject or of the rights and freedoms of others.”

\(^{138}\) Recital 27 Directive 95/46/EC.

\(^{139}\) In the case of split tasks, the person determining the purposes of the processing is the controller (D. De Bot (2001). Verwerking van Persoonsgegevens. Antwerpen: Kluwer).
As the person responsible for the execution of the processing and the person conducting the actual processing are not necessarily the same, the directive foresees the possibility of a processor. This is:

…a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Note that the processor has to be a person external to the controller. If, for instance, the controller is a company and it designates one of its employees to perform the processing, this employee is an internal designate and no external processor. The processor therefore performs the processing on behalf – but not under direct authority – of the controller. The distinction between processor and controller is not always very clear.

Controller versus processor

Although the classification as a controller or processor is highly important to determine the precise scope of the responsibilities and liabilities of a certain party to the processing, the distinction between these two notions is not always very clear and well defined. For data protection it will therefore be essential to establish a clear distinction between these two actors and their respective roles.

As defined under the general introduction to the key principles of Directive 95/46/EC, the controller is the natural or legal person who holds the authority to determine the purposes and the means of the processing of personal data. In case of a legal person, the employees of this legal person concerned with handling the data that is to be processed – or even performing the actual processing – are considered as internal designates. If the controller, however, assigns the task of processing the personal data to an external entity, to execute the processing on the controller’s behalf, then said external entity is considered to be a processor.

From these definitions, one can understand that the main characteristic of the controller is to ‘determine the means and purposes’ of the processing, while the processor executes ‘on behalf of the controller’. The mere application of these definitions can already lead to discussion, as the attribution of the authority to determine means and purposes or of the ability to act on behalf of another party may to a certain extent lie in the eye of the beholder. Therefore, the attribution of control or of delegation to one or another party may be subject to the person or entity performing such attribution.

Recent technological and societal developments have also influenced these two concepts and their applicability. At the time of the drafting of Directive 95/46/EC, the EU envisioned very specific models of data processing that allowed for a more clear-cut application of the concepts of controller and processor. The rise of the Internet, with new communication models and means for service providing, has led to the creation of new data processing models that allow for

---

140 Note for instance article 6 (2) of Directive 95/46/EC indicating that it is the responsibility – and thus the liability – of the controller to ensure that the general principles of fair and lawful data processing are observed.

141 Although the legal term ‘delegation’ can be understood broader than is intended here, the term is used in order to follow the precise wordings of the Article 29 Working Party.

a less static attribution of the concepts of control and delegation, therefore making it difficult to establish the roles of controller and processor. This may even lead to the appointment of co-controllers, leading to joint liability.\footnote{Ibid.} Joint control may in turn lead to even greater confusion regarding the precise division of liabilities between these joint controllers and even applicable law.\footnote{Ibid.} As service providers are ever more convergent, one entity may in one aspect of its tasks be a controller, while being a processor in other aspects of his tasks.

The Article 29 Working Party has taken notice of the changing times and the consequences thereof for the application of the concepts of controller and processor. In an opinion, the Working Party aims to give an overview of the current situation, as well as an attempt to allocate responsibility to ensure compliance.\footnote{Article 29 Working Party (2010). Opinion 1/2010 on the concepts of "controller" and "processor". WP 169.} The Working Party sees it as “the crucial challenge […] to provide sufficient clarity to allow and ensure effective application and compliance in practice”.\footnote{Ibid.}

On the other hand, continued effectiveness needs to be ensured and undue consequences under changing circumstances need to be avoided by balancing the need for present acceptable consequences with future needs for adjustment.

Regarding the issue of control, the Working Party determines that this is a factual issue that can be assessed pragmatically with a view to ensure predictability.\footnote{Ibid.} The Working Party distinguishes three situations from which control can stem: from explicit legal competence, from implicit competence and from factual influence.

Regarding the means and purposes of the processing of personal data, the Article 29 Working Party states that, in short, this refers to the why and how of the processing.\footnote{Ibid.} In assessing who determines purposes and means, it will be important to maintain a pragmatic approach, looking into the level of influence a certain party exercises. After all, a processor will, up to a certain extent, determine the means for the processing, as he performs the actual processing. The mere fact that he has some level of determination on the means for the processing does, however, not automatically qualify him as a controller. The level of discretion is therefore the key component in assessing the ability of determination, and therefore in attributing the role of controller.

On the issue of joint control, the Article 29 Working Party wants to ensure that the ever more complicating data processing models of today do not hinder an easy and efficient allocation of roles and responsibilities. Full compliance to data protection principles should be ensured at all

\begin{footnotesize}
\begin{enumerate}
\item[Ibid.]\footnotetext{Article 4 (1) (a) of Directive 95/46/EC states that the law of the territory in which the controller has its main establishment is applicable to the processing.}
\item[Ibid.\textsuperscript{145}]\footnotetext{Article 29 Working Party (2010). Opinion 1/2010 on the concepts of "controller" and "processor". WP 169.}
\item[Ibid.\textsuperscript{146}]\footnotetext{Ibid.}
\item[Ibid.\textsuperscript{147}]\footnotetext{Ibid.}
\item[Ibid.\textsuperscript{148}]\footnotetext{Ibid.}
\item[Ibid.\textsuperscript{149}]\footnotetext{I.e. when the controller or the specific criteria for his nomination are designated by national or Community law.}
\item[Ibid.\textsuperscript{150}]\footnotetext{I.e. when the capacity to control has not been explicitly laid down by law, but can be derived from common legal provisions or established legal practice pertaining to different areas.}
\item[Ibid.\textsuperscript{151}]\footnotetext{I.e. by analysis of contractual relations between parties involved.}
\item[Ibid.\textsuperscript{152}]\footnotetext{Article 29 Working Party (2010). Opinion 1/2010 on the concepts of "controller" and "processor". WP 169.}
\item[Ibid.\textsuperscript{153}]\footnotetext{Note that the Article 29 Working Party has a broad view on the concept of means. This not only includes deciding upon the actual technical measures of processing the data, but also certain organizational measures such as deciding upon which data is to be processed, which third parties can gain access to the data, which data is to be deleted, etc. As the determination of the means is to a certain extent the task of the processor, this broad definition sensitively enlarges the scope of the processor’s work package. Determination of purpose, however, is reserved to the controller.}
\end{enumerate}
\end{footnotesize}
times, even in the case of a controller whose limited role prohibits from fulfilling his full duties as a controller.

The Article 29 Working Party therefore aims to allocate responsibility where the actual control is exercised, making the concept of controller more of a functional concept, than a mere static one. Although this opinion is a laudable attempt at providing more clarity on the applicability of the concepts of controller and processor to a highly different environment than which they were originally intended for, the opinion still leaves a number of underlying issues untouched. For one, regarding the issue of co-control, the Working party stresses the need for a clear allocation of roles. In this respect it should be noted that (co-)controller contracts could provide a clear division of tasks and responsibilities and could therefore provide for an effective role allocation. Such contracts are, however, still not legally recognized. Introducing the requirement for controllers to draft such contracts in order to ensure compliance in the EU legal framework on data protection could therefore already lead to a much clearer role division, thereby providing a solution to the main issues regarding role and responsibility attribution.

Regardless of the Article 29 Working Party opinion, the application of the concepts of controller and processor to new data processing models still leaves room for legal uncertainty. One can therefore look forward to the upcoming review of Directive 95/46/EC to see how these concepts and their application will evolve.

**Actors**

The EXPERIMEDIA project will have to carry out an analysis of the relevant actors participating in various scenarios, to specify their roles and to define their rights and obligations. Special focus should be given on the specification of the data controller, as this will be of fundamental importance for the determination of the national applicable legislation.

**Third party**

A third party is:

…any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

This definition is by default negatively formulated: any entity that is no controller, processor or data subject is by definition a third party.

**Recipient**

A recipient is a:

…natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.
This is any person to whom the personal data is disclosed. Such disclosure can be interpreted very broad, as making the personal data available – for instance through a website – can also constitute a potential disclosure. Note that in principle every entity can be a recipient, which includes controller, processor and third party. Employees of the legal person/controller receiving access to the personal data are internal recipients.

**Consent**

**Introduction**

Finally, the article provides a definition for the data subject’s consent. This is:

...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

This consent can be given both explicitly as implicitly.\(^{154}\) Although the directive does not specify that consent needs to be granted in writing, a written and signed consent form is obviously preferred from an evidential point of view. The fact that the consent needs to be given freely indicates that it cannot be given as a result of external pressure, for instance emanating from the controller. Furthermore, consent can only be given for a specific processing. Therefore, no consent can be given for all future processing of personal data. The consent also needs to be informed, meaning that the data subject needs to be well aware of the means and purposes of the processing for which he grants his consent. The data subject can at any time revoke his consent ex nunc, therefore disabling the use of his data for future processing. The revocation of consent for a past processing is not possible.

**How to obtain the data subject’s consent?**

The data subject’s consent is an important notion in the processing of personal data.\(^{155}\) Also for the processing of sensitive personal data, the data subject’s consent is one of the few cases in which such processing can be performed.\(^{156}\) It should be noted though, that consent is certainly not the only way for conducting a legitimate processing of personal data, even sensitive personal data. As Member States can enlarge the cases in which personal data can legitimately be processed or the exceptions in which sensitive personal data can be processed, it becomes clear that the data subject’s consent will not be required for a fair degree of processing. However, the vast majority of the cases will still require the data subject’s consent as the cases of article 7 and the exceptions of article 8 of Directive 95/46/EC are still rather narrow and allow for relatively little application, even when enlarged in national implementation by the Member States.

As indicated earlier, the consent can be given both explicitly and implicitly. Important is that the consent is given freely, without external influence, aimed at a specific processing. Furthermore, the consent needs to be informed\(^{157}\), meaning that the data subject needs to be well aware of the means and purposes of the processing for which he grants his consent. Although the directive

\(^{154}\) In the case of split tasks, the person determining the purposes of the processing is the controller (D. De Bot (2001). Verwerking van Persoonsgegevens. Antwerpen: Kluwer, 403p.)

\(^{155}\) Article 7 (a) Directive 95/46/EC.

\(^{156}\) Article 8 (2) (a) Directive 95/46/EC.

itself does not state that consent needs to be provided in writing, it is clear that from an evidential point of view written consent will always be preferred. In certain cases, written consent will be mandatory, for instance in certain national implementations of the provisions of the directive. As national implementations of the Directive – and thus of the concept of consent – may differ, certain Member States may impose more thorough requirements on how the data subject’s consent can be provided.

Although it may not seem an easy task to ask each data subject involved in a certain processing of personal data for his consent, it does serve a dual purpose. While the consent enables the data controller to perform his envisioned data processing in a legitimate manner, the fact that he needs to inform the data subject before this party can make his informed decision, could also serve as compliance to the duty to inform the data subject.

The most common way of receiving consent is using a consent form. Such form provides the data subject with all the information he needs to know before making his free, specific and informed decision on granting his consent to the processing of his personal data. The idea is that the data subject carefully reads the consent form before signing it and handing it back to the data controller. In practice, however, the use of consent forms could lead to certain issues.

One issue with using consent forms is that they are more often than not based on standard forms that are barely edited to fit the specific cause they serve. If a consent form provides only a general repetition of the data subject’s rights, which could be copied directly from Directive 95/46/EC, the data subject will still not be well informed to provide his consent to the processing at hand. One can therefore recommend that consent forms need to be drafted with care to ensure that the data subject becomes fully aware of the processing for which his consent is sought, its actors, its means and purposes and which personal data is required for such processing. Only in such case, a signed form can indicate compliance to the duty to inform the data subject, as well as the clear and written consent of the data subject to the processing of his personal data.

It is, however, no easy task to draft a clear and informative consent form. To make the data subject fully aware of the precise nuances involved in the processing at hand, the actors and their precise roles and the exact means and purposes of the processing, requires precise drafting that will more often than not result in a long and tedious text unintelligible to all people but lawyers. One will therefore have to find a compromise between the need for the consent form to be precise and complete and the request for user friendliness.

An unintelligible text may read to the refusal of the data subject to sign the form as he does not comprehend what is laid out before him, but it may also go by unnoticed. Although consent is an important principle in the field of data protection – after all it provides the data subject with the power to personally determine which of his personal data can be processed in which processing – it seems to have lost some of its original strength. In the current society, data subjects need to

---

158 For instance in processing sensitive and medical personal data in Belgium, written consent is mandatory: Articles 6 and 8 Belgian Privacy Act.
159 Article 10 Directive 95/46/EC.
160 Many standard templates for consent forms or even consent form generators can be found on the Internet.
provide their consent on a daily basis for a plethora of services.\textsuperscript{161} As a result, a majority of data subjects has become conditioned to signing consent forms and currently does so without bothering to look what the contents of the form are.\textsuperscript{162} The threshold for providing consent to a specific processing of his personal data has become so low that the very use of such consent forms may certainly be questioned.

It is therefore recommended to draft clear consent forms that invite the data subject to actually read them instead of blindly signing them and to monitor whether the data subject has really understood what is conveyed to him in the consent form.\textsuperscript{163}

\begin{center}
\textbf{Consent in EXPERIMEDIA}
\end{center}

Given the nature of the experiments services, informed consent would be the most viable justification ground for the processing of the personal data. The participants in the experiments should be provided with a —preferably— written consent form by the EXPERIMEDIA consortium. Consent should be revocable and should also be regularly renewed, thus limiting the validity of consent in time. The users should be made aware when geolocation services are activated, for instance by a visible icon. By default, such services should be switched off.

\subsection{5.2.1.2. Basic principles of processing}

Three principles form the basis of every fair and lawful processing: Legality/transparency, finality and proportionality.\textsuperscript{164}

\textit{Legality/transparency}

The principle of legality means that the data subject needs to reasonably know which of his personal data is processed, why and by whom. If a public legal entity processes personal data, it needs to provide a clear legal norm as basis for the processing. For private persons — natural and legal — this means that sufficient transparency on the purposes and means of the processing needs to be provided. Specifically, the directive states that data can only be processed if:

\begin{itemize}
\item[(a)] the data subject has unambiguously given his consent; or
\item[(b)] processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
\item[(c)] processing is necessary for compliance with a legal obligation to which the controller is subject; or
\end{itemize}

\textsuperscript{161} Installing software, creating an account on a website, etc. The number of examples in which personal data is processed is countless and virtually all of these examples require the data subject’s consent.

\textsuperscript{162} Especially on the Internet, the simple ‘click to accept’-button has lowered the threshold to providing consent even further.

\textsuperscript{163} The need for stronger and clearer rules on informed consent was also addressed by the Commission: Communication of 4 November 2010 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “A comprehensive approach on personal data protection in the European Union”, COM(2010) 609, 8-9.

\textsuperscript{164} Articles 5, 6 and 7 Directive 95/46/EC.
(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) [of the Directive].

**Finality**

No fair and lawful processing can be performed without clearly delineating specified, explicit and legitimate purposes. The purposes need to be disclosed to the data subject and need to be adequately formulated in order for him to give his informed consent. Data can also not be further processed in a way incompatible with those purposes.\(^{165}\)

**Proportionality**

Data need to be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed. They may not be stored longer than is necessary for the purposes for which the data were collected or for which they are further processed.\(^{166}\) Data needs to be accurate and, where necessary, kept up to date. Inaccurate or incomplete data needs to be erased or rectified.

Although the principle of proportionality is not directly mentioned in Directive 95/46/EC and can only be vaguely deduced from article 6 of the directive, it is one of the cornerstones for fair and lawful processing of personal data. The principle of proportionality is even considered a cornerstone for EU community law and is included in the Treaty on the European Union.\(^ {167}\) In summary, this principle entails a two-tiered assessment.\(^ {168}\) First, one needs to establish whether the proposed means are adequate to achieve the envisioned purpose. Second, one needs to assess whether the proposed means will lead to negative consequences on interests protected by law and whether such negative consequences can be justified in the light of the envisioned purpose. The goal of such assessment is to ensure whether there is no other means available that would lead to the same result, but would lead to less negative consequences.

The principle of proportionality could therefore be regarded as a principle of minimization. In choosing the means for the processing of personal data, the principle of proportionality requires one to choose the ‘lesser of two evils’. As the data collected may also not be excessive “in

---

\(^{165}\) Note that further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible.

\(^{166}\) This corresponds to the idea of data minimization.


\(^{168}\) Other authors describe a trie-tiered process: suitability (Are the means suited to reach the purposes?), necessity (Are the means necessary to meet the purposes?) and non-excessiveness (Do the means not go further than what is strictly necessary to attain the purposes?). L.A. Bygrave, D.W. Schartum (2009). Consent, proportionality and collective power”. in S. Gurwirth et al. (eds.). Reinventing data protection?. Springer, 162.
relation to the purposes for which they are collected and/or further processed”, the principle of proportionality could also be regarded as referring to the concept of data minimization. Processing excessive amounts of data would therefore be considered as a violation of the principle of proportionality.

The principle of proportionality, as general principle of basic EU community law and as one of the main principles of the EU legal framework on data protection, will therefore have to be complied with in all processing of personal data.

As can be deduced already from this summary overview of the core components of the principle of proportionality and their implications, this will require a certain degree of planning up front.\textsuperscript{169} For instance, if the principle of proportionality dictates that the means used in the envisioned processing of personal data may not be excessive to the purposes of said processing, then one will obviously have to decide on the proportionality of the means at the moment those means are decided upon. Any post factum assessment of the proportionality of the means used will be too late, as the potential violation of the proportionality principle will have already occurred.

Therefore, if a certain processing of personal data is planned, one will have to decide on a number of issues at the very moment of determining the means that will be used to execute the envisioned processing. The means will often – at least to a certain degree – be decided upon by the processor, rather than the controller. In this regard, one could think of reaching an agreement between controller and processor regarding the means to be used for the processing.\textsuperscript{170} Such agreement will be of high importance, as a controller will want to avoid allowing his processor to decide upon the means he will use to execute the processing and subsequently deciding upon means that are excessive to the purposes set forth by the controller. It is, after all, the responsibility of the controller to ensure that all data processing is carried out fair and lawful, which includes complying with the principle of proportionality.

Second, the personal data that is to be processed in the envisioned data processing needs to be exhaustively determined on beforehand in order to ensure that no more data is collected than is absolutely necessary to meet the purposes set forth by the controller.

Regarding those purposes it should be noted that these might not be exceeded, as stated in article 6 (1) (c) of Directive 95/46/EC.


\textsuperscript{170} As indicated earlier, the directive does currently not require such agreements, but as the relationship between (co-)controllers and processors becomes of ever-increasing importance to the allocation responsibilities and liabilities in processing personal data, one can expect such agreements to attain a more recognized position after the planned review of Directive 95/46/EC.
5.2.1.3. Data subject’s rights

Right to information

The controller needs to provide certain information to the data subject. A distinction is made between the situation where the controller receives the data from the data subject personally or from another source.

If the information has been obtained from the data subject, in so far as such further information is necessary:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as: the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him.

If the information has been obtained from another source, in so far as such further information is necessary, and with the exception of processing for statistical purposes or for the purposes of historical or scientific research, or if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him.

Right of access

The data subject has the right to exercise a certain degree of control over his personal data. First of all, he may ask for confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed. He may also ask communication to him in an intelligible form of the data undergoing processing and of any available information as to their source and knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions. This information needs to be supplied to him without constraint at reasonable intervals and without excessive delay or expense.

---

171 Articles 10 and 11 Directive 95/46/EC.
172 Article 12 Directive 95/46/EC.
Right to correction

The data subject may also ask – where appropriate – the rectification, erasure or blocking of data of which the processing does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.\(^\text{173}\) This includes notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the data subject’s request for correction, unless this proves impossible or involves a disproportionate effort.

Right to object

On compelling legitimate grounds relating to his particular situation, the data subject has the right to object to certain types of processing.\(^\text{174}\) The directive lists “processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority and processing necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed” as cases in which the right to objection needs to be granted. Furthermore, he can object to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

5.2.1.4. Special categories of data

The processing of personal data is in principle allowed if the processing complies with the principles of fair and lawful processing. Article 8 of the directive, however, defines special categories of data of which the processing is prohibited. Specifically, this concerns “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.” Summarized, article 8 prohibits the processing of sensitive data, medical data and judicial data.

There are, however, a number of exceptions that do allow for the processing of these special categories of data:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject’s giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a

\(^{173}\) Article 12 Directive 95/46/EC.

\(^{174}\) Article 14 Directive 95/46/EC.
political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(c) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.\footnote{175}{Article 8 (3) Directive 95/46/EC.}

Article 8 (3) provides an exception for processing required for preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Article 8 (5) provides an exception for processing of data relating to offences, criminal convictions or security measures. These may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

5.2.1.5. Confidentiality and security

The directive also provides for the confidentiality and security of the processed personal data.\footnote{176}{Articles 16 and 17 Directive 95/46/EC.} These are technical and organizational measures that need to lead to more secure processing and storage of personal data. Even in an otherwise strictly fair and lawful processing, data leakage could cause an infraction to the principle of data minimization.

Article 16 concerns the persons acting under the authority of the controller and the processor. They may not process the personal data except on instructions from the controller, unless he is required to do so by law. This ensures confidentiality.

Article 17 deals with the security of the processing. Member States need to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. For implementing measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, the state of the art and the cost of their implementation will be taken into account.

The controller needs to ensure that the processor can provide sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out. The controller must also ensure compliance with those measures. The duties of the processor need to be governed by a contract or legal act binding the processor to the controller and stipulating that the processor shall act only on instructions from the controller, and that the
controller’s obligations shall also be incumbent on the processor. For evidential matters, such contract or legal act needs to be concluded in writing.

5.2.1.6. Notification

In order to assess whether a certain processing complies with the principles set forth by the directive, a duty of notification has been included in article 18 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. Member States can, however, simplify the notification or provide exemptions for a number of reasons listed under article 18 (2). Most notably, this includes the appointment of a personal data protection official.

Regarding the content of the notification, article 19 states that this includes:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

The Member States must also determine which type of processing can bear specific risks for the personal rights and freedoms and must ensure that these types of processing are examined prior to their start. The national supervisory authority will perform such examination.

Finally, the Member States need to adopt measures to guarantee the publicity of the processing operations. National supervisory authorities will keep a public register of duly notified processing operations. Also processing operations exempt from the duty of notification need to supply the information included in article 19.

5.2.1.7. Data transfers

In principle, processed personal data can only be transferred to a third State if such State can guarantee an adequate level of data protection. This adequacy is assessed in the light of all the circumstances surrounding a data transfer operation, in particular “the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.” The Commission performs such assessment. Article 26 provides a number of

177 Article 25 Directive 95/46/EC.
exceptions to this rule of data transfer. These exceptions are formulated in the same line as the exceptions to the principal prohibition of processing special categories of data.

5.2.1.8. Supervisory authority

Within each Member State, one or more independent public legal entities will monitor the implementation and the national application of the principles set forth in the directive. Next to an advisory function, these supervisory authorities are granted powers of investigation, the power to intervene and the power to engage in legal proceedings.\textsuperscript{178} Given the nature of their tasks, the members of the supervisory authorities are sworn to secrecy.

Representatives of the national supervisory authorities are united in the so-called Article 29 Working Party. This Working Party acts as a pan-European advisor and strives for a more harmonized and coherent application of the principles of the directive throughout the EU Member States. Its precise tasks are listed under article 30.

5.2.2. Location based services

\textit{Introduction}

The ePrivacy directive contains specific provisions for the processing of location data that are not needed for the purpose of the conveyance of a communication or for the billing thereof (“location data other than traffic data”) and are processed for the provision of value added services\textsuperscript{179} that are based on the location of the user. Such value added services are commonly known as location based services and cover for instance services that provide the users with traffic information or, as in the EXPERIMEDIA Schladming scenario, offer guidance to visitors recommending spots recommended by other visitors\textsuperscript{180}.

\textit{Processing of location data}

Article 9 of the ePrivacy Directive regulates the processing of such location data for the provision of value added services:

```
1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.
```

Within the protective ambit of Article 9 of the ePrivacy Directive, location data other than traffic data relating to users or subscribers of public communications networks or publicly available

\textsuperscript{178} Article 28 Directive 95/46/EC.
\textsuperscript{179} Value added services are defined in Article 2(g) of the ePrivacy Directive as “any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof”.
\textsuperscript{180} Recital 35 2002 ePrivacy Directive.
\textsuperscript{181} Article 9(1) ePrivacy Directive.
electronic communications services that are used for the provision of a location based service may be processed only when they are made anonymous, or when the users or subscribers have given their consent to the provision of such a location based service. In any case, the location data may only be used to the extent and for the duration necessary for the provision of the value added service. The users and the subscribers should be given the opportunity to withdraw their consent for the processing of the location data at any time. The withdrawal will be valid for the future. The users and the subscribers should also be offered the choice to temporarily refuse the processing of their location data for each connection to the network or for each transmission of a communication, using simple means and free of charge. This can for instance be done via a switch on/off option of the terminal equipment.

The processing of location data may be undertaken only by persons acting under the authority of the network operator, the service provider or the third party providing the value added service and only for the purposes of providing the value added service. It should be pointed out that while the obligations relating to the processing of location data for the provision of value added services cover only the mobile operators (or the electronic communications operators in general), the third parties that are involved with the provision the value added service on the basis of location data that they receive from the mobile operators are bound by the obligations arising from the Data Protection Directive.

Schladming – Location data of visitors

The technologies mentioned in Schladming scenario are not only intended to be used as a means for data transfer. They can also be used for geolocation and tracking purposes. Location data of visitors are used for the provision of location based services, such as the suggestion of a detour in order to see the gallery that other visitors have recommended. Besides the protection vested by the Data Protection Directive on the processing of personal data of the visitors, the ePrivacy Directive contains specific provisions for the processing of location data for the provision of location based services. The consent of the users should be obtained for the processing of their location data.

5.2.3. National privacy legislation

Being a directive, the principles of Directive 95/46/EC discussed here first need to be transposed into the national legal system of the EU Member States. Unlike a regulation, directives are not self-executing and are thus not immediately enforceable as law in the Member States. As directives only provide a certain goal that needs to be met and usually leave it to the Member States to decide upon the means they wish to adopt to achieve said goals, it is of no surprise that the national implementation of directives can lead to very divergent results.

---

183 Article 9(1) ePrivacy Directive.
184 Article 9(1) ePrivacy Directive.
185 Article 9(2) ePrivacy Directive.
186 Article 9(3) ePrivacy Directive.
187 ARTICLE 29 DATA PROTECTION WORKING PARTY, ‘Opinion on the use of location data with a view to providing value added services, WP115’ (2005), p. 4
A directive is therefore by nature not the most ideal legal instrument if one aims to create a pan-European harmonized framework on a certain topic. This has become very apparent in the case of the EU legal framework on data protection, as found by Directive 95/46/EC. The initial purpose of the Directive was not so much to block the processing of personal data, but to facilitate data transfers between the EU Member States. Such data transfers were at that time severely restricted due to the highly divergent national privacy policies of the Member States. The directive was therefore aimed at supporting the further expansion of the common market and introducing a harmonized level of data protection throughout the whole EU. Harmonizing elements can, for instance, be found in article 1 (2) that states that Member States “shall neither restrict nor prohibit the free flow of personal data between Member States” for reasons connected with the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.\(^\text{188}\)

Although one could argue that the directive has attempted to provide harmonization on this topic, the clear divergence in Member States’ policies shows that the effect of the directive has remained limited to the establishment of a minimal degree of protection. Certain parts of the directive – such as article 5, article 8 (7) and recital 9 – allow for a degree of national differentiation that goes beyond what could be expected from a true attempt at harmonization. If harmonization was the true goal of the principles of Directive 95/46/EC, this goal may have been missed by utilizing a directive and by allowing for such a high degree of national differentiation.

The divergence of national policies on data protection could also hinder the goal of facilitating data transfers between the EU Member States. As, for instance, the national supervisory authority in one Member State holds up higher demands for notifications than the national supervisory authority in another Member State, the transfer of data between these Member States may be hindered. The Article 29 Working Party has taken note of these divergences and has issued opinions and recommendations for a more coherent interpretation across the EU. Examples of this include Opinion 1/2010 on the concepts of "controller" and "processor" and Opinion 4/2007 on the concept of personal data.

**Specification of the applicable national data protection legislation**

As different EU Member States may have divergent national provisions regarding data protection, the EXPERIMEDIA consortium will have to specify the data controller in each of the experiments and to define what would be applicable national data protection legislation(s) to the processing of personal data of the users.

Due notification to the competent national Data Protection Authority (or Authorities), in compliance with national legislation, is required.

**5.2.4. Review of Directive 95/46/EC**

Even though the data protection directive was adopted in 1995, the grand majority of the principles therein are directly taken from the Council of Europe’s 1981 Convention for the

Protection of Individuals with regard to Automatic Processing of Personal Data. With thirty years of use and remaining virtually unchanged, one could therefore wonder whether the main principles that, to this day, form the basis of the legal framework of EU data protection should be replaced by newer principles that better reflect the drastically changing nature of data communication and data protection. Current issues – the Internet, social media, etc. – were not around at the time that these principles were conceived and their authors could not possibly have foreseen the drastic changes to the information society in the past decade.

At this moment, outdated principles are applied to situations they were never intended to be applied to; this leads one to wonder when the limits of the flexibility of these principles will finally be reached. The need for a thorough review of Directive 95/46/EC can therefore no longer be ignored. Even the opinions of the Article 29 Working Party may have reached their limits as their legal value may be contested, as they may push interpretations of existing principles too far and as they may not always provide more coherence in such interpretations. A new approach therefore seems imperative to render the current legal framework on EU data protection more future proof.

A number of issues to be discussed during the review of Directive 95/46/EC include the basic definitions found in article 2. Growing discussion on the scope and interpretation of notions such as controller, processor, personal data and sensitive data have demonstrated the need for reform. With regards to the right to information, criticism has risen on standardized privacy policies often found on websites. Although such generic privacy policies may comply with the requirements set forth by the directive, they do not necessarily provide the data subject with the information he really needs, therefore not meeting the purpose of the right to information.

Apart from reviewing existing principles, a number of new principles may be added to the next iteration of the EU data protection framework. For one, it is clear that in the information society it has become very difficult to permanently erase data. Many websites provide links to content found on other websites, while others even copy certain content to their own servers. Because of the large scale on which this linking and copying takes place, it is virtually impossible to compile an exhaustive list of which web servers offer a certain piece of information. If said piece of information concerns the personal data of a data subject, he may face an insurmountable challenge in having this information deleted from the internet permanently. To counter what can be referred to as the perpetual memory of the internet, one could think of a right to be forgotten as complement to the right to privacy, traditionally referred to as the “right to be let alone”. Such would enable the data subject to personally determine that their data is no longer processed and deleted when they are no longer needed for legitimate purposes.

---

190 The Commission has addressed this principle as such: Communication of 4 November 2010 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “A comprehensive approach on personal data protection in the European Union”, COM(2010) 609, 7-8.
191 A proposal for a law providing a “right to be forgotten” has already been introduced in the French Senate: “Au total, il convient de noter que plusieurs mesures de la présente proposition de loi permettent de donner une plus grande effectivité au droit à l’oubli numérique”; Sénat France, Proposition de Loi visant à mieux garantir le droit à la vie privée à l’heure du numérique, www.senat.fr, 2009-2010, nr. 93.
Another means for enhancing the data subject’s control over his own personal data is the notion of data portability.\textsuperscript{192} Such would allow the data subject to fully withdraw his personal data from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers.

Another idea coined by the Commission is to establish a right to silence of the chips.\textsuperscript{193} This would give the data subject the right to disconnect from their networked environment at any time.

The possibility of review was discussed in July 2010 during a meeting of the Article 29 Working Party.\textsuperscript{194} It was discussed that national supervisory authorities should receive a more important role in supervising the application of the EU data protection framework. Regarding the review of the principles of the directive, the French Commission Nationale de l’Informatique et des Libertés (CNIL) warned that such review could entail a lengthy procedure.\textsuperscript{195}

\textsuperscript{192} Also addressed in: Communication of 4 November 2010 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “A comprehensive approach on personal data protection in the European Union”, COM(2010) 609, 7-8.

\textsuperscript{193} Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, “Internet of Things — An action plan for Europe”, COM(2009) 278, 5-6.

\textsuperscript{194} ec.europa.eu/justice/policies/privacy/news/docs/pr_15_07_10_en.pdf.

6. Liability issues

6.1. Liability of service providers

6.1.1. Introduction

EU provisions on liability can be found in a plethora of different legal instruments. One of such instruments is the Directive on e-commerce, which contains specific provisions dealing with the liability of service providers.\(^{196}\)

Specifically, this directive refers to the liability of intermediary service providers.\(^{197}\) The main idea behind these provisions can be found in a basic problem created by the Internet. As the Internet can be used as a means to circulate harmful or illegal information it is important to assess who can be held liable for such information. In many cases, however, it will not be an easy task to identify the user that uploaded the information. As a result, such cases are often redirected towards the service provider that hosted the website on which the information was posted or the internet service provider that provides the internet access to the user suspected of uploading the harmful or illegal information. As it may lead to undesirable effects to hold service providers liable for all acts committed by the users of their services, the EU has created a specific framework that governs the liability of these intermediary service providers. The provisions in the directive on liability cover three specific situations and provide a final general provision.

The EU saw such provisions necessary to ensure that no unreasonable burden was put on the intermediary service providers as they play an important role in the development of the Internet and e-commerce, particularly in cross-border transactions. The provisions of the directive relating to these liability issues were therefore almost literally transposed into national law by the Member States.\(^{198}\) Although the directive only addressed the three situations discussed earlier, certain Member States have even further expanded this waiver of liability to hyperlinks and search engines.\(^{199}\)

6.1.2. Mere conduit

First, the directive addresses the situation of mere conduit.\(^{200}\) This means that, when a service provider only transmits the information provided by a recipient of the service, or only provides access to a communication network, this service provider will not be held liable for that transmission. Such is, however, subject to the conditions that the service provider

(a) does not initiate the transmission;

---


\(^{197}\) Articles 12 to 15 Directive 2000/31/EC.


\(^{199}\) Ibid., 13.

\(^{200}\) Article 12 Directive 2000/31/EC.
(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.\(^{204}\)

Even if such information transmission or access provision would include automatic, intermediate and transient storage, such storage would still be regarded as mere conduit if it is conducted for the sole purpose of transmitting information and if the information is not stored for a longer period than necessary for the transmission.\(^{202}\) Although service providers can under the scope of this provision not be held liable for the nature of the information transmitted, they can be asked to terminate or to prevent an infringement.\(^{203}\)

### 6.1.3. Caching

A second situation addressed by the directive is that of caching.\(^{204}\) In the same vein as the provision on mere conduit, service providers are not held liable for the automatic, intermediate and temporary storage of information, if such storage is performed for the sole purpose of making the further transmission of said information to other requesting users more efficient. Also here, this is subject to certain conditions, namely that the service provider

(a) does not modify the information;

(b) complies with conditions on access to the information;

(c) complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;

(d) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and

(e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.\(^{205}\)

As under the previous article, while not held liable, service providers can be asked to terminate or to prevent an infringement.\(^{206}\)

### 6.1.4. Hosting

The third specific situation addressed by the directive is hosting.\(^{207}\) If a service provider delivers the service of storing information provided by the recipient of the service, the service provider will not be held liable for the contents of such information. This is, however, subject to the conditions that the service provider

\(^{201}\) Article 12 (1) Directive 2000/31/EC.
\(^{202}\) Article 12 (2) Directive 2000/31/EC.
\(^{203}\) Article 12 (3) Directive 2000/31/EC.
\(^{204}\) Article 13 Directive 2000/31/EC.
\(^{205}\) Article 13 (1) Directive 2000/31/EC.
\(^{206}\) Article 13 (2) Directive 2000/31/EC.
\(^{207}\) Article 14 Directive 2000/31/EC.
(a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.\(^{208}\)

Furthermore, the service provider may not control or exercise authority over the recipient of the service and he may still be required to remove the information or block access thereto.\(^{209}\)

The European legislator probably did not foresee the emergence of web 2.0 technology and of new media players taking up the role of new intermediaries. But today we can observe a tendency to broaden the exemption of purely technological players to these new platform operators. Intermediaries such as MySpace, forum keepers or even bloggers providing third parties with a virtual space where they can upload and store their own content have with varying degrees of success made use of the exemption as hosting providers, provided there was no prior moderation, selection of content producers or other active intervention in the content uploaded by the users.\(^{210}\)

6.1.5. No general obligation to monitor

Lastly, the directive provides that one cannot ask the service providers to monitor all information transmitted or stored by them or to actively locate illegalities therein.\(^{211}\) If service providers are made aware of alleged illegalities concerning the information they transmit or store, they will need to inform the appropriate authorities.\(^{212}\)

Schladming - User-generated video streaming and sharing

The issue of the liability of service providers is important for the experiment in Schladming. Visitors of Schladming are stimulated to upload audiovisual content or pictures of their journey (user generated content - UGC) at Schladming on YouTube like or Facebook like service. It is obvious that every user is responsible for the content he uploads. However, the question rises whether the service provider of the Schladming YouTube like and Facebook like services could also be held liable for the information uploaded by users. If the service provider could be labelled as a host, it will not be held liable if the two conditions are cumulatively met: 1) the service provider may not have actual knowledge of illegal activity or information, 2) the service provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. Given that the service provider does not actively select the content and does not control its organisation in a chronological schedule or a catalogue and only offers a portal and platform to users to upload their audiovisual content, it is doubtful that it will have actual knowledge of illegal activity or information.

\(^{208}\) Article 14 (1) Directive 2000/31/EC.

\(^{209}\) Article 14 (2) and (3) Directive 2000/31/EC.


\(^{211}\) Article 15 (1) Directive 2000/31/EC.

\(^{212}\) Article 15 (2) Directive 2000/31/EC.
Furthermore, the service provider can remove, ex post and acting upon complaints, illegal content for the platform. The service provider does not have a general obligation to actively monitor all content on its platform.

6.2. Liability under data protection regulations

Parties involved in the processing of personal data may face liability under the EU legal framework on privacy and data protection. In particular, this concerns the data controller and data processor. As these two main actors in the topic of personal data processing have divergent responsibilities, it is essential to clearly demarcate the precise roles of these two actors.

The main provisions regarding the processing of personal data found under article 6 of Directive 95/46/EC must be complied with in each processing of personal data. The same article states that it is the responsibility of the data controller to ensure such compliance.\(^{213}\) Likewise, it is the responsibility of the data controller to ensure that the rights of the data subject are respected and that they can be effectively exercised.\(^{214}\) Further responsibilities of the data controller include the confidentiality and security of the processing and notification to the appropriate Data Protection Authority (DPA).

Given the importance of the role of the data controller in the processing of personal data, the EU has decided to include provisions on remedies, liability and sanctions in the directive. Regarding remedies, the directive refers to the possibility of administrative remedies before inter alia the national DPA.\(^{215}\) Such national DPA could, for instance, provide the data subject with assistance in the exercise of his rights in the processing of his personal data for purposes of national security or defence.\(^{216}\) The national DPA could also intervene in legal proceedings against a processing that does not comply with existing legislation. Apart from intervening in legal proceedings launched by others – mainly data subjects whose rights were violated – national DPAs could also independently engage in legal proceedings when the principles of the national legal framework on data protection have been violated. The directive also provides that Member States must ensure that access to the national judicial authority is cleared for any breach of the rights guaranteed to him by national legislation applicable to the processing.

With regards to liability, the directive provides that “any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.”\(^{217}\)

Once more, this provision clearly points to the controller as the person liable for all damages resulting from incompliant processing. The controller may be exempted – partially or wholly – if

\(^{213}\) Article 6 (2) Directive 95/46/EC.
\(^{214}\) Articles 10 to 12 and 14 Directive 95/46/EC.
\(^{215}\) Article 22 Directive 95/46/EC.
\(^{216}\) Article 28 Directive 95/46/EC.
\(^{217}\) Article 23 Directive 95/46/EC.
he can provide evidence that he was not responsible for the event that gave rise to the damage. This provision bears resemblance to the general Aquilian liability and the tort of negligence.\textsuperscript{218}

Lastly, the directive provides that Member States must “lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive”.\textsuperscript{219} Such sanctions could be rather steep. The Belgian Privacy Act, for instance, includes fines up to € 100,000 and up to two years of prison sentence for repeated offences against the provisions included in the Act.\textsuperscript{220}

As can be concluded from this overview, the data controller faces strict liabilities under the EU legal framework on privacy and data protection. When processing personal data, it will therefore be of capital importance to ensure that all principles of the applicable national data protection legislation(s) are duly complied with.

\section*{All experiments}

It is important that the controllers of the processing of personal data are specified for each of the scenarios not only to ensure that they fulfil the rights of the data subject, but also that they are held liable in cases of incompliant or illegal processing of personal data.

---

\textsuperscript{218} Note that the article illustrates that three elements similar to those found in the Aquilian liability are present: “damage resulting from an unlawful processing operation” indicates the elements of damage, causality and a certain degree of fault, as the processing must be unlawful. It is, however, not the person suffering the damage that will have to prove the data controller’s wrongdoings. Contrarily, it is the data controller himself that needs to provide proof of his not being responsible for the damages suffered. This lends a certain degree of objectivity to the provision in the directive.

\textsuperscript{219} Article 24 Directive 95/46/EC.

\textsuperscript{220} Articles 37 to 43 Belgian Privacy Act.
7. Conclusion

All of the legal requirements presented above have to be taken into account by the EXPERIMEDIA project. Fulfilment of these requirements is necessary to ensure legal compliance of the different experiments with the regulatory framework. These requirements will be consolidated and completed here.

BASIC DATA PROTECTION REQUIREMENTS

- Actors identified as data controllers must be aware of the precise definitions of national data protection legislation applicable to the processing under their control. Collaboration with the competent national Data Protection Authority will ensure a correct understanding of the specific national implementation of the definitions of the applicable notions.
- The data subject’s free, informed, specific and unambiguous consent must be obtained for legitimate processing of personal data. While such consent is only one of the possible justification grounds for legitimate personal data processing, it will in most cases be the only viable justification ground for personal data processing with relation to the EXPERIMEDIA experiments. (Further on consent, see infra)
- Fair and lawful processing of personal data must demonstrate legality or transparency.
- The purposes of the processing of personal data must be clearly indicated in advance.
- The processing of personal data may only include relevant and non-excessive data, in relation to the specified purposes. Data must be collected for a specified, explicit and legitimate purpose and may not be further processed in a way incompatible with those purposes. Duration of data storage must be limited and stored data must be destructed once the purpose for which that data was collected has been attained.
- Data minimization can also be achieved by employing methods for anonymisation or pseudonymisation of personal data. Here, data unlinkability should be kept in mind as linkability could lead to the identification of a particular data subject.
- The data controller must ensure sufficient information of the data subject.
- The data controller must ensure that the data subject can fully enforce his right of access, his right to correction and his right to object.
- The data controller must ensure confidentiality and security of the processing of personal data under his control.
- Due notification must be made to the competent national Data Protection Authority (or Authorities), in compliance with national legislation.
- Data transfers to third States must comply with applicable legislation.

CONSENT REQUIREMENTS

- Carefully drafted privacy policies and consent forms must ensure compliance to the requirement of consent and the right to information. Note that such privacy policies and consent forms must be compliant with national data protection legislation. For instance,
certain jurisdictions require written consent, while others allow for implicit consent in many cases.

- User-friendliness should be the focal point in obtaining the data subject’s consent. While unintelligible texts may lead to the data subject not reading a privacy policy or consent form, elaborate procedures to grant consent may result in the data subject refraining from using such service, thus damaging the business of the data controller. A balance between the interests of both parties should therefore be struck.

- When dealing with minors, elderly and/or persons with a mental illness, the data controller is advised to seek consent from both the data subject and its statutory or legal guardians. The general legal capacity of the data subject determines its capacity to consent.

- Informed consent must be given freely. In order to determine whether the data subject’s consent was given freely, one must analyse the external pressure exercised on his decision. Positive persuasion cannot invalidate his freely given consent, while negative coercion will invalidate his consent as it could not have been given freely.

- Consent should be limited in time and should be renewed for continuously on-going processing of personal data. Consent should also be revocable.

CONFIDENTIALITY AND SECURITY

- In the processing of personal data, the data controller must restrict access to this personal data to the persons that need such access for the processing they perform under his authority. Such access need to comply with the proportionality principle, meaning that no user may be awarded access to more data than strictly required for his processing tasks.

- In order to achieve proportional access control, the data controller must provide for differentiated access levels for different user groups in order to ensure proportionality. This must be combined with an access procedure that includes registration, identification, authentication and authorization.

- In the processing of personal data, the data controller must adopt appropriate and state of the art technical and organizational measures to ensure data security. Also the processor must be bound to such security policy.

- Such security policy should include, inter alia, actions to be taken in case of data breach, the use of cryptography to protect data and audit trails to log and trace data access and use. These security policies should also take into account user-friendliness and should require minimal user effort. When using audit trails, the data controller must define the purposes and scope of this logging and make transparent who can access these logs as audit trails constitute personal data processing.

- While previous requirements only apply in the context of the processing of personal data, adherence thereto in other cases of security and access management is strongly recommended as they provide valuable minimal requirements.

- Regardless of the technology used, the data subject should be made fully aware of the presence of the technology and of its activities and of the possibility for deactivation.
• As geolocation data must be viewed as personal data, the processing thereof must comply with the principles of the Data Protection Directive and its national implementations.

• Prior informed consent must be obtained for the processing of geolocation data, as this will mostly be the only viable justification ground for the processing of this data. This consent must be revocable and must be regularly renewed.

• Geolocation services should be switched off by default. The user should be made aware of active geolocation services. The user should also be given the option to choose the granularity of his consent. The user should also be given the option to opt-out from databases containing Wi-Fi access points.

CONTENT REGULATION REQUIREMENTS

• Media service providers having editorial responsibility should take into account the obligations included in the AVMS Directive.

• Platform operators, such as YouTube-like services, do not fall under the scope of the AVMS Directive, because they don’t have editorial responsibility.

COPYRIGHT

• A very wide range of works are copyright protected when the necessary criteria are fulfilled. A creation needs to be original in order to receive protection.

• Users may not upload copyright protected content on UGC-platforms.

• It is not clear whether the routines of synchronised swimming will be copyright protected. While most of sports games lack any originality, a choreography of synchronised swimming requires a certain level of originality in order to arrange the movements in a specific sequence.

LIABILITY

• A service provider that could be labelled as a host will not be held liable if the two conditions are cumulatively met: 1) the service provider may not have actual knowledge of illegal activity or information, 2) the service provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

• The service provider does not have a general obligation to actively monitor all content on its platform.

• Controllers of the processing of personal data could be held liable in cases of incompliant or illegal processing of personal data.