

SEVENTH FRAMEWORK PROGRAMME

“Information Society Technologies”



**Deliverable D7.4**  
**Legal evaluation report**

**Project acronym:** +Spaces

**Project full title:** Policy Simulation in Virtual Spaces

**Contract no.:** 248726

<b>Workpackage:</b>		WP7
<b>Editor:</b>	Eleni Kosta	KU Leuven
<b>Author(s):</b>	Eleni Kosta Fanny Coudert Dimitris Koryzis Aleksandra Kuczerawy	KU Leuven KU Leuven HeP KU Leuven
<b>Authorized by</b>	Kostas Tserpes	NTUA
<b>Doc Ref:</b>	D7.4	
<b>Reviewer</b>	Dimitris Koryzis	Hellenic Parliament
<b>Reviewer</b>	Ilias Spais	ATC
<b>Dissemination Level</b>	Public	

## Executive Summary

This deliverable carries out an evaluation of the legal and ethical issues that were researched within the +Spaces project, steered by the legal developments within Europe, as well as by the actual needs of the project and pilots.

More specifically this deliverable presents the experiences of the +Spaces consortium from the analysis of the Terms and Conditions of virtual spaces, with which the +Spaces prototype had to be interoperable, i.e. Facebook, Twitter, Blogger and OpenWonderland. The analyses of the aforementioned documents influences technical choices and decisions that had to be made by the consortium in various areas relating to (a) posting content, (b) deploying user interface, (c) storing content and (d) extracting content.

As the privacy of the users and protection of their personal data is valued very high by the +Spaces consortium, +Spaces made an extensive analysis of the legal requirements stemming from the data protection legislation. This deliverable documents in detail the issues that were identified and the way how the +Spaces consortium chose to deal with them.

Finally, as the relevant national legislation to be applied to the +Spaces prototype is the Greek one and as the partner that represented the end users in the +Spaces consortium was the Hellenic Parliament (HeP), the Greek legislative system is briefly presented and the possible use of +Spaces tools in the legislative procedure is discussed.

## Table of Contents

1	Introduction.....	5
2	Towards the building of the +Spaces platform .....	6
	2.1 Introduction to Terms and Conditions of virtual spaces .....	6
	2.2 Compliance with T&C.....	10
	2.3 The +Spaces experience from the analysis of the Terms and Conditions of virtual spaces.....	11
3	Data processing in +Spaces .....	13
	3.1 Introduction.....	13
	3.2 Controller/processor- role definition .....	13
	3.3 Applicability of the Data Protection Directive and definition of applicable law .....	15
	3.3.1 Household exemption .....	15
	3.3.2 The applicability of the Data Protection Directive on the processing of pseudonymous data .....	16
	3.3.3 Definition of applicable national legislation.....	17
	3.4 Definition of an appropriate legal basis .....	17
	3.4.1 Consent as the legal basis in +Spaces.....	17
	3.4.2 Information to be given to the data subject .....	19
	3.4.3 Some thoughts on the acquisition of user consent in the frame of research projects.....	21
	3.5 Ensuring fairness and transparency of the data processing activities .....	22
	3.6 Definition of the purpose of the processing.....	23
	3.7 Data minimisation principle .....	23
	3.8 Collection of sensitive data .....	24
	3.9 Conservation of the data.....	25
	3.10 Ensuring the accuracy of the data.....	26
	3.11 Rights of the data subjects .....	26
	3.12 Confidentiality of the data .....	27
	3.13 International transfers of personal data .....	28
	3.14 Notification of the processing to the competent Data Protection Authority .....	28
4	Legal evaluation of +Spaces in Greece .....	28
	4.1 Legislative process in Greece .....	28

4.2	Procedures of Parliamentary Control.....	29
4.3	Interesting Means of Parliamentary Control.....	30
4.4	Possible Use of +Spaces tools in the legislative procedure.....	30
5	Conclusions.....	32
6	Annex I: Controller/processor agreements.....	34
7	Annex II: Full version of the +Spaces privacy notice.....	45
8	Annex III: +Spaces condensed privacy notice.....	49
9	Annex IV: +Spaces Terms of Use.....	51
	Terms of Use of the +Spaces Platform.....	51
10	Annex V: Report +Spaces/WeGov Workshop.....	57

## 1 Introduction

Deliverable 2.3 “Ethical issues report” was prepared in the first six months of the project and aimed at the identification of legal issues that were foreseen to arise within the +Spaces project, mainly focusing on privacy and data protection. More specifically, that deliverable provided an overview of legal obligations stemming from the data protection legal and regulatory framework that would need to be complied with, when the +Spaces prototype would process personal data of users. Moreover, it identified privacy issues and it formulated some first legal requirements directed to the technical partners and compiled a number of research questions that could be the topic of legal research during the project.

+Spaces, like every European research project is a dynamic project. The consortium commenced from the first requirements that were identified in Deliverable 2.3, but it soon had to both expand into the investigation of new requirements that arose in the design and development phase of the prototype, as well as to set some of the research questions aside those that were identified in the beginning of the project as potentially relevant.

An example of the former dealing with the investigation of new requirements relates to the analysis of the Terms and Conditions on which the +Spaces platform would be working. The need for such an analysis became obvious as it was deemed crucial for the consortium to not only develop a functional +Spaces prototype, but to ensure that the prototype would be also legally compliant and wouldn't violate the terms and conditions of the virtual spaces it was using for its developments, i.e. Facebook, Twitter, Blogger and OpenWonderland. This very careful analysis fed important requirements and it influenced the shaping of specific functionalities of the +Spaces prototype. +Spaces has been, to our knowledge, the first European research project that carried out such a detailed analysis of Terms and Conditions, in partial collaboration with the Soclos project (Exploring Social Networks for Building the Future Internet of Services) that carried out a similar exercise. Section 2 of this deliverable contains a description of this experience hoping to provide valuable insight to other European research projects.

The latter case relates to research questions that had to be put aside, although they were identified in the beginning of the project as potentially relevant. The data protection legislation prohibits transfers of personal data to third countries unless these countries provide for an adequate level of protection. In the beginning of the project it was discussed whether personal data of +Spaces users would be sent to Israel (IBM) for analysis. Israel has been acknowledged as providing an adequate level of protection by the Commission Decision 2011/61/EU of 31 January 2011, meaning that no additional safeguards to the ones usually required for transfers of personal data to any other Member States were required<sup>1</sup>. However, the consortium decided to avoid the transfer of personal data outside the European Union and the Data extraction would take place on NTUA servers, based in Athens. This choice of the +Spaces consortium, which was driven by the wish to offer

---

<sup>1</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:en:PDF>

maximum protection to the users, rendered the further investigation of the legal issues relating to the transfer of data to third countries not very crucial and relevant.

Section 3 of this deliverable contains an analysis of the data protection requirements that stem from the relevant data protection legislation and should be complied with by the +Spaces prototype. This section is largely based on the structure that was followed in Deliverable 2.3. It describes issues that had to be taken into account in order to draw specific legal requirements and it explains choices of the +Spaces consortium that influenced technical functionalities of the prototype as well the formation of the privacy notice of the project, as well as its terms of use.<sup>2</sup>

Finally, as the relevant national legislation to be applied to the +Spaces prototype is the Greek one and as the partner that represented the end users in the +Spaces consortium was the Hellenic Parliament (HeP), the Greek legislative system is briefly presented and the possible use of +Spaces tools in the legislative procedure is discussed.

## **2 Towards the building of the +Spaces platform**

### **2.1 Introduction to Terms and Conditions of virtual spaces**

The +Spaced prototype is not a stand-alone system that could be stored for example on an external device and be used by any user. The +Spaces prototype is building on existing virtual spaces, and more specifically on Facebook, Twitter, Blogger and OpenWonderland, the platforms of which it uses in order to deploy the +Spaces polls and debates. This means that the +Spaces project had to ensure that the prototype that would be built, as well as the pilots that would be carried out for its testing, should not only be interoperable with these platforms, but should also respect and be compliant with their Terms and Conditions.

These Terms and Conditions (T&C's), sometimes also called Terms of Service, are addressed to all entities that interact with the virtual world: users, programmers or application developers. In practice, there are different version of T&C's for users on the one hand and for developers/application providers on the other. The main reason for such distinction is that the traditional users in general provide content while the developers also extract content through the platform's application programming interfaces (APIs).

The T&C's provide a list of rules under which the developers, who want to build applications on existing virtual spaces, are allowed to use the API of the virtual space in order to access and exploit such content. In other words, T&C's "describe the policies and philosophy around what type of innovation is permitted with the content and information shared on"<sup>3</sup> a particular virtual space. They are sometimes called "a letter of law of the platform"<sup>4</sup>.

T&C's represent a legal agreement between the provider of the virtual space and any developer or programmer interested in building an application that would utilize content available on this space through its APIs. In fact, they are considered to be a contract, in

---

<sup>2</sup> Both documents are Annexed in this deliverable.

<sup>3</sup> Twitter Developer Rules of the Road, <https://dev.twitter.com/terms/api-terms>

<sup>4</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>

which one side is the virtual space provider and the other is the application developer. This contract outlines the rights, obligations and limitations of the application developer as well as the warranties and disclaimers made by the platform provider with regards to the platform.

The contract is entered into by accession, which means that there is no requirement for the developer to express his explicit consent to the given rules. By using the platform, his consent is automatically inferred. Moreover, the interested developer must ensure that the service or product he plans to introduce complies with all the described conditions. The virtual space provider usually assigns itself a power to monitor the way the developers use its API to ensure that this is the case. In case the virtual space provider discovers that the developer has attempted to exceed or circumvent the given limitations, his ability to use the API and its content may be blocked, temporarily or even permanently.<sup>5</sup>

This means that even though T&C's are considered to be a contractual agreement, there is no negotiation process in which both parties express their wishes or concerns. To the contrary, T&C's, which govern basically every aspect of the provider-developer relation, are determined by the virtual space providers in their complete discretion. This could be described as a 'take-it-or-leave-it' situation, as all the power rests on one side of the contract.

Moreover, the provider of the virtual space often reserves the right to completely change, or redesign the given rules along the way. Typically no prior notification is deemed necessary, although the recent trend is to announce the upcoming changes publically, for instance through a blog post<sup>6</sup>. In its T&C's, Twitter specifies that "the Rules will evolve along with our ecosystem as developers continue to innovate and find new, creative ways to use the Twitter API, so please check back periodically to see the most current version". Facebook is even more straightforward about its ability to implement changes without notice, stating that they "can change these Platform Policies at any time without prior notice as we deem necessary. Your continued use of Platform constitutes acceptance of those changes"<sup>7</sup>. This could possibly lead to a situation when a developer finds himself in violation of the given rules because he did not check them for a period of time and they have changed dramatically since he first introduced his product.

T&C's consist of a set of conditions and requirements regulating how the application developers can interact with and leverage the content of the virtual space. The rules they contain are usually very extensive and provide very detailed specifications. They address issues like extracting content, posting content, communication with the users, their privacy, or transfers of data to third parties, etc. The rules have a technical but also legal nature. In combination they create a full image of the philosophy of the virtual space on accessing and exploiting its content.

---

<sup>5</sup> Twitter Developer Rules of the Road, <https://dev.twitter.com/terms/api-terms>

<sup>6</sup> Sippey M., Changes coming in Version 1.1 of the Twitter API, at <https://dev.twitter.com/blog/changes-coming-to-twitter-api>.

<sup>7</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>

It is generally advisable that the examination of the terms and conditions is conducted by a legal partner and a technical partner, in a close cooperation with each other. During such joint analysis the legal partner is able to explain the legal requirements and what legislation they are a result of. This is the situation mainly with regard to the privacy and data protection related terms, but also intellectual property rights. An example of such term, in Facebook, is: "Subject to certain restrictions, including on transfer, users give you their basic account information when they connect with your application. For all other data obtained through use of the Facebook API, you must obtain explicit consent from the user who provided the data to us before using it for any purpose other than displaying it back to the user on your application"<sup>8</sup>. In Twitter, an example of such term is: "Respect the privacy and sharing settings of Twitter Content. Do not share, or encourage or facilitate the sharing of protected Twitter Content. Promptly change your treatment of Twitter Content (for example, deletions, modifications, and sharing options) as changes are reported through the Twitter API"<sup>9</sup>. Within +Spaces there was an excellent collaboration between technical and legal partners in order to achieve the best possible result for the development of the +Spaces prototype and its functionalities.

In the area of intellectual property rights Facebook's policies provide that "In the United States you must take all steps required to fall within the applicable safe harbors of the Digital Millennium Copyright Act including designating an agent to receive notices of claimed infringement, instituting a repeat infringer termination policy and implementing a "notice and takedown" process. In other countries, you must comply with local copyright laws and implement an appropriate "notice and takedown" process upon receiving a notice of claimed infringement". This provision requires a prompt reaction to the notification of an infringement through an adoption of the specific "notice and take down" procedures from the applicable national law.

At the same time T&C's contain a large number of strictly technical requirements, like for example: "End users must be presented with the option to log into Twitter via the OAuth protocol. End users without a Twitter account should be given the opportunity to create a new Twitter account as provided by Twitter. You must display the Connect with Twitter option at least as prominently as the most prominent of any other third party social networking sign-up or sign-in marks and branding appearing on you Service"<sup>10</sup>. Another example would be "Your website must offer an explicit "Log Out" option that also logs the user out of Facebook"<sup>11</sup>.

In both cases, the technical solutions, which need to be implemented, have to be designed by the technical partners. In the compliance assessment it is the technical execution of the conditions that will matter most. It is therefore the comprehension of the terms by technical partners that will have a crucial impact on the level of compliance with T&C's.

---

<sup>8</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>

<sup>9</sup> Twitter Developer Rules of the Road, <https://dev.twitter.com/terms/api-terms>

<sup>10</sup> Twitter Developer Rules of the Road, <https://dev.twitter.com/terms/api-terms>

<sup>11</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>



The goal of these rules, in the first place, is to protect the business of the virtual space provider. After all, a provider of any such space is a for-profit company. As such, it has its own business interests that it needs to protect from anyone whose business model might be in conflict with theirs. This could be the case when an application profits too much from the freely accessible content of the virtual space and becomes too popular. In such situation it could become a direct competitor and will be seen as a threat to the platform's interests. In order to prevent this outcome, platform providers introduce rules and limitations for developers. The situation is however not static, as new applications are constantly developed with creative ways of using content available in virtual spaces. For this reason the providers of the virtual spaces continue to adjust the rules and make them stricter. Twitter admits, any of its "updates and modifications may adversely affect how your Service accesses or communicates with the Twitter API. If any change is unacceptable to you, your only recourse is to terminate this agreement by ceasing all use of the Twitter API and Twitter Content. Your continued access or use of the Twitter API or any Twitter Content will constitute binding acceptance of the change"<sup>12</sup>.

The providers of the virtual spaces need to monitor closely the application ecosystem. They achieve that by demanding that the developers cooperate with them, especially in case the application requires a large amount of API calls. According to Twitter "One of the key things we've learned over the past few years is that when developers begin to demand an increasingly high volume of API calls, we can guide them toward areas of value for users and their businesses. To that end, and similar to some other companies, we will require you to work with us directly if you believe your application will need more than one million individual user tokens"<sup>13</sup>. Facebook, on the other hand, is more explicit in its statement that once an application makes a serious impact in the ecosystem, more stringent rules will apply: "If you exceed, or plan to exceed, any of the following thresholds please contact us as you may be subject to additional terms: (>5M MAU) or (>100M API calls per day) or (>50M impressions per day)"<sup>14</sup>.

Within the main goal of protecting its business it is possible to distinguish a secondary goal, which is the protection of the traditional users of virtual spaces whose content will be reused by the application. This side of the platforms' protectiveness contributes to the transparency and fairness of the activities of the virtual spaces' providers towards their users. After all, these users are not always aware how the external applications process their data. By introducing certain limitations, these providers actively defend users' interests, particularly in the area of privacy protection and intellectual property rights. The example of such term would be the requirement for use consent, as it will be described in "3.4 Definition of an appropriate legal basis". This requirement allows for more control of the personal data by the users and is in line with the on-going review of the Data Protection Directive. The main incentive of such protective behaviour, very often, is an attempt to avoid a possible vicarious liability for the developers' activities. Nevertheless, the effect that the

---

<sup>12</sup> Twitter Developer Rules of the Road, <https://dev.twitter.com/terms/api-terms>

<sup>13</sup> Michael Sippey: Changes coming in Version 1.1 of the Twitter API, at <https://dev.twitter.com/blog/changes-coming-to-twitter-api>.

<sup>14</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>

stringent rules have on the overall protection of the users' interests should not be diminished.

## 2.2 Compliance with T&C

All the aspects described above prove that compliance with the T&C's of the platform should be given proper attention, from the design phase of an application. This task should be definitely treated as seriously as the actual development process.

First of all, one of the main problems encountered by the developers refers to the interpretation of the terms. The rules are drafted unilaterally, and they are also subject to the exclusive interpretation of the platform provider. As Facebook states in their T&C's: "We can take enforcement action against you and any or all of your applications if we determine in our sole judgment that you or your application violates Facebook Platform Terms and Policies"<sup>15</sup>. In other words, it is entirely up to them to decide who is playing by their rules and who is not. Such phrasing clearly indicates that the platform provider is not interested in considering any interpretation of its rules that would differ from their perspective. Their view, however, is usually not presented to the public. Some explanation might be provided but it seldom is exhaustive enough to clarify all the doubts.

This can be particularly problematic in case of provisions that are phrased in a vague manner. An example of such term could be one from the recent Twitter updates, stating that: "No other social or 3rd party actions may be attached to a Tweet". With no additional explanation on what is meant by a "3<sup>rd</sup> party action", and whether email clients ("Email link") and web browsers ("Open in Safari") would count as such, this wording created a state of panic among the developers.<sup>16</sup>

By keeping their cards close to their chest, platform providers guarantee they have an upper hand in case of any conflict, since there is no possibility to contest their opinion. There is a strong chance that all the ambiguities with regard to the understanding of the provisions will be resolved to the disadvantage of the application developer. This could happen even if he truly tried to comply with a term, but unfortunately for him, did not achieve the result satisfactory to the provider of the virtual space. The result is that "effectively, Twitter can decide your app is breaking a (potentially vague) rule at any time, or they can add a new rule that your app inadvertently breaks, and revoke your API access at any time"<sup>17</sup>.

Another factor complicating *bona fide* attempts of compliance is the frequency of changes to the T&C's. As shown above, providers of virtual spaces reserve themselves a right to rewrite the given conditions anytime, and any way, they feel it is required. This means the rules can change from one day to another, possibly without any warning. Additionally, possible future changes are very difficult to predict. They reflect the business interest of the platform providers which are the most urgent to protect, but there is no possibility to foresee their nature or the extent of thereof. This is of course within their prerogative as the owner of the

---

<sup>15</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>

<sup>16</sup> Arment M., Interpreting some of Twitter's API changes, 16 August 2012, <http://www.marco.org/2012/08/16/twitter-api-changes>

<sup>17</sup> Arment M., Interpreting some of Twitter's API changes, 16 August 2012, <http://www.marco.org/2012/08/16/twitter-api-changes>

space. However, it creates a grave difficulty for the developers who can never be sure if their application continues to comply with all the standards. This makes T&C's very unstable and unpredictable; offering no assurance as to whether something will be permitted in the future.<sup>18</sup> The existence of the applications is therefore always very precarious.

The only option the developers have, is to re-assess their application every time an update is announced. In case of a problem, he has a choice between re-designing the application or its certain functionalities or drop it completely. As a result, the compliance control is a never ending process from which the developer can never retire if he wants his application to continue existing. This means, "that anyone who builds a product on a third-party platform, especially a free one, risks losing everything, anytime, on a moment's notice".<sup>19</sup>

All these aspects of compliance with T&C's are equally relevant for the research projects. There are no exceptions created for research activities, which would make the situation of a research project any easier. As can be imagined, the continuous changes and re-assessments can lead to serious delays of the project. The only solution that the research projects are left with is to contact the targeted platform provider and enquire about special conditions for scientific purposes. There is however no guarantee that such exception will be granted.

### **2.3 The +Spaces experience from the analysis of the Terms and Conditions of virtual spaces**

In the course of the development of the +Spaces project, the consortium dedicated significant amount of time and efforts in carrying out a thorough analysis of the Terms and Conditions of the various spaces that are used by the project for the running of the +Spaces platform, both the ones that are addressed to users, as well as the ones addresses to developers/application providers. In this way the consortium carefully studied the potential implications for +Spaces and ensured full compliance of our system to the relevant European and national legal framework. To our knowledge +Spaces has been the first European funded research project to carry out such detailed research, in partial collaboration with the Soclos project (Exploring Social Networks for Building the Future Internet of Services) that carried out a similar exercise.

The provisions of the Terms and Conditions of Facebook, Blogger, Twitter and OpenWonderland that were crucial for the +Spaces prototype can be classified into four categories: (a) posting content, (b) deploying user interface, (c) storing content and (d) extracting content.

---

<sup>18</sup> Arment M., Interpreting some of Twitter's API changes, 16 August 2012, <http://www.marco.org/2012/08/16/twitter-api-changes>

<sup>19</sup> Phelps A., Twitter's API changes will have a real impact on news developers, Nieman Journalism Lab, 17 August 2012, [http://www.niemanlab.org/2012/08/twitters-api-changes-will-have-a-real-impact-on-news-developers/?utm\\_source=Weekly+Lab+email+list&utm\\_campaign=650bc81e79-WEEKLY\\_EMAIL&utm\\_medium=email](http://www.niemanlab.org/2012/08/twitters-api-changes-will-have-a-real-impact-on-news-developers/?utm_source=Weekly+Lab+email+list&utm_campaign=650bc81e79-WEEKLY_EMAIL&utm_medium=email)

The +Spaces platform posts content onto the spaces on behalf of the policy makers, by actually deploying the experiments, by posting questions and background information for the debates and by soliciting participation through the use of its Twitter and Facebook accounts of the users. As far the posting of content is concerned, +Spaces consortium had to analyse, interpret and comply with terms of T&C's relating to the issuing of one sided press releases from various spaces on the use of their platform by +Spaces, as well as with issues relating to intellectual property rights linked to the posted content. The adaptors of +Spaces deploy user interfaces on the various spaces in the form of applications that engage citizens in +Spaces experiments. In relation to such deployment of user interface, +Spaces consortium dealt with issues that could arise from limitations in the linking to or redirecting of users to competitive sites.<sup>20</sup> In order to comply with such a requirements, the +Spaces consortium had to modify the way how recommendations work, returning only experiments within the same space, although this may be considered as actual weakening of the recommendation service. Another term that was taken into account in the design of the +Spaces prototype was the fact that some spaces required an option that also logs the user out of the virtual space, not only from the +Spaces interface<sup>21</sup>.

As part of its functionalities, the +Spaces platform stores information from the various spaces that is posted by citizens as a response to a +Spaces experiment invitation.. Obviously, issues with regard to the protection of privacy of the users and on the processing of their personal data arose at this point. The +Spaces consortium took great care in ensuring that the privacy of the users is respected at all times and in complying with the relevant legislation on data protection, as it is further elaborated in section 3.

The last category of terms related to the extracting of content, as the +Spaces platform extracts information from the various spaces at various instances. User data are transferred to various components (middleware, services) that may reside on servers of different partners in different countries. Moreover, the information is analysed and some of the results are sent back and presented on the spaces, for example in the form of recommendations. In the design and implementation of the relevant functionalities, the relevant terms of the T&C's had to be taken into account, as they could be introducing limitations on transferring content to other contexts or limitations relating to copyright.

The compliance with the Terms and Conditions of all aforementioned social networks and virtual spaces (Facebook, Twitter, Blogger, OpenWonderland) has proven a challenging task. On the one hand, each platform had specific particularities and all of them had to be taken into account for the design and the implementation of the +Spaces prototype. On the other hand the Terms and Conditions can (and do) change without any notification, a fact that requires constant re-evaluation and assessment of technical components. An extensive description of the analysis that was carried out in the course of the +Spaces project would not contribute much value to future European research projects, as they will not only have to always check whether the relevant terms and conditions have been modified, but they

---

<sup>20</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>

<sup>21</sup> Facebook Platform Policies: <http://developers.facebook.com/policy/>

would also have to carefully study the terms that will be of special importance for their own needs.

Moreover, during analysis of the T&C's in a research project partners have to take into account different risk management approaches that each partner follows internally. At a consortium level, in which various partners need to cooperate and adopt a single policy regarding risk management, the task of identifying how the research and development undertaken during the project complies with the T&Cs, is a matter of internal discussion and separate agreements. Even though these procedures infuse a great overhead in the work, in fact they are necessary in order to ensure perfect compliance with and policy alignment to internal rules of each of the partners.

In any case, European research projects should be aware of the wide effect the T&C's might have on the planned architectures and changes that may be required in order to comply with them. For this reason, the necessary examination and thorough analysis should be undertaken as early in the project's lifecycle as possible.

## **3 Data processing in +Spaces**

### **3.1 Introduction**

Deliverable 2.3 "Ethical issues report" was prepared in the first six months of the project and aimed at the identification of legal issues that were foreseen to arise within the +Spaces project, mainly focusing on privacy and data protection. More specifically, that deliverable provided an overview of legal obligations stemming from the data protection legal and regulatory framework that would need to be complied with, when the +Spaces prototype would process personal data of users. As the privacy of the users and protection of their personal data is valued very high by the +Spaces consortium, +Spaces made an extensive analysis of the legal requirements stemming from the data protection legislation during the whole duration of the project. This deliverable documents in detail the issues that were identified and the way how the +Spaces consortium chose to deal with them.

This section contains an analysis of the relevant applicable legislation, the definition of the roles of the +Spaces partners in the context of data processing, the specification of the purposes for which data processing activities took place in +Spaces, the obligations of the data controller relating to the quality of the data, the rights of the data subject, notification to the supervisory authority. The +Spaces consortium developed a number of documents (full and condensed privacy notice, agreements between data controller and data processors, terms of use of the +Spaces platform), that are Annexed to this deliverable. Important for the analysis was the opinion of the Greek DPA on the COCKPIT project which touched upon some of the issues that also had to be dealt with in the +Spaces project.

### **3.2 Controller/processor- role definition**

The identification of actors who are present in the processing of personal data and the definition of their rights and obligations is important for any research project, such as

+Spaces. The structure of European research projects **challenges the role of the data protection actors**, i.e. the data controller and the data processor. A data controller is “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data[...]”<sup>22</sup>. A data processor is “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller”<sup>23</sup>.

The classification of a natural/legal person as ‘data controller’ or ‘data processor’ is of great importance for several issues, such as who shall carry the obligations appointed to the ‘data controller’ by the Data Protection Directive and who is to define the details of the data processing. As a rule of thumb it can be said that the data controller is liable for violations of the Data Protection legislation, while the role of the data processor is reduced<sup>24</sup>. Moreover, the specification of the data controller is very important, as the applicable national legislation will be defined based on the Member State where the data controller has its establishment (see section 3.3, below).

As several partners are involved in the design of the system, the development of the architecture and the deployment of the +Spaces platform, it has been difficult to define who will be the responsible for the processing of the personal data of the users of the +Spaces platform, i.e the data controller (see Figure 1).

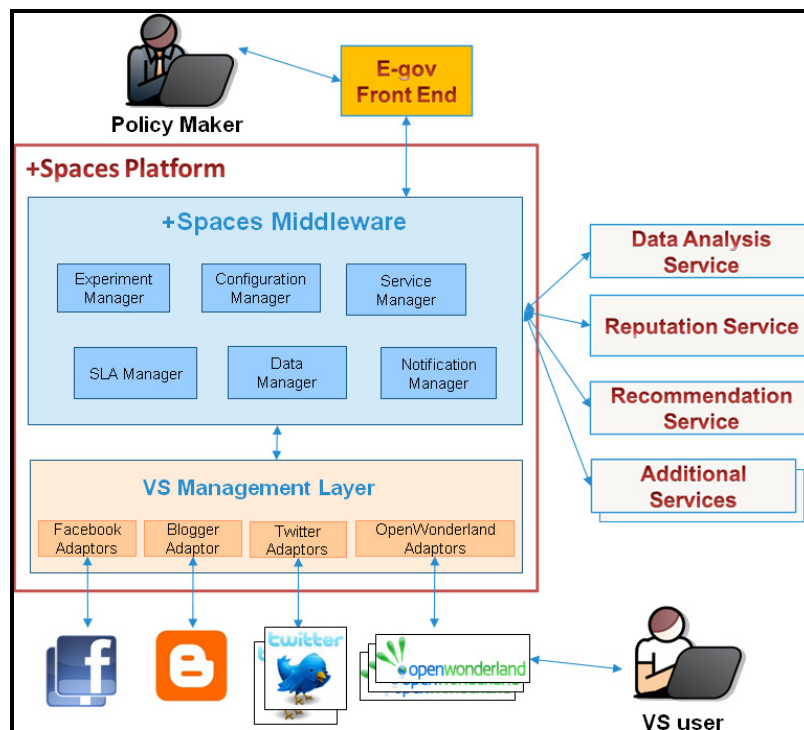


Figure 1: +Spaces architecture

<sup>22</sup> Article 2(d) Data Protection Directive and Article 2(g) Greek Data Protection Law.

<sup>23</sup> Article 2(e) Data protection Directive and Article 2(h) Greek Data Protection Law.

<sup>24</sup> Kuner, C., *European Data Privacy Law and Online Business*, Oxford University Press, 2003, p.62

In a very simplified way, it could be said for example that within the +Spaces project ATC was responsible for the front-end, NTUA for the back-end, the data extraction and some other services, while Fraunhofer was responsible for the data analysis service. From a strictly technocratic point of view, the +Spaces consortium as a whole should ideally be determined as the data controller, as all the choices are made collectively and the consortium functions as a group. However, as the +Spaces consortium, exactly like every other consortium of European research projects, does not have legal personality, it could not be determined as data controller. Alternatively, the various partners of the +Spaces consortium that are established in various Member States and participate to a lesser or larger extent to the processing of the user data, should be determined as joint controllers (co-controllers). However, this would entail a huge administrative burden and would require the investment of large resources for the carrying out of the administration linked to the appointment of co-controllers that would be impossible to realise, due to the time and budget restrictions that exist in the project.

In order to solve this problem, the consortium took some technical decision in order to make the role of some partners more distinct, for instance the data extraction took place on the NTUA servers, located in Athens, instead of the IBM premises in Israel. A separate licencing agreement was signed between IBM and NTUA. The partner ATC, established in Athens, was declared data controller, while NTUA and Fraunhofer were defined as data controllers. Dedicated controller-processor agreements were duly signed between ATC and NTUA on the one hand, and ATC and Fraunhofer on the other, as required by the data protection legislation. These agreements can be found in Annex I: Controller/processor agreements” of this deliverable. ATC has been consistently mentioned as data controller in the relevant consent forms that were linked to the +Spaces pilots (see below section 3.4.2), as well as in the +Spaces privacy notice, shown in Figure 2.<sup>25</sup>

<p><b>About the organization responsible for the organization of the +Spaces pilot (‘ data controller’)</b></p> <p>+Spaces Consortium partner Athens Technology Center (ATC) (Rizariou 10, Chalandri 152 33, Athens, Greece, Tel:+30/210-6874300, Fax: +30/210-6855564, e-mail: info-spaces@atc.gr , is the responsible for the organization of the +Spaces Pilots.</p>
---

Figure 2: ATC as data controller in the +Spaces privacy notice

## 3.3 Applicability of the Data Protection Directive and definition of applicable law

### 3.3.1 Household exemption

Especially with regard to research on social networking sites, there is a lot of **confusion on whether the Data Protection Directive is applicable to the users of such sites or the “household exemption”<sup>26</sup>** applies. The Article 29 Working Party in its opinion on online social networking tried to shed some light on this issue:

<sup>25</sup> See Annex II: Full version of the +Spaces privacy notice”.

<sup>26</sup> Art. 3(2), second indent Data Protection Directive and Art. 3(2) Greek Data Protection Law .

*“Typically, access to data (profile data, postings, stories...) contributed by a user is limited to self-selected contacts. In some cases however, users may acquire a high number of third party contacts, some of whom he may not actually know. A high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller. [...]When access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines, access goes beyond the personal or household sphere. Equally, if a user takes an informed decision to extend access beyond self-selected ‘friends’ data controller responsibilities come into force. Effectively, the same legal regime will then apply as when any person uses other technology platforms to publish personal data on the web<sup>9</sup>. In several Member States, the lack of access restrictions (thus the public character) means the Data Protection Directive applies in terms of the internet user acquiring data controller responsibilities”<sup>27</sup>.*

However, this approach does not clarify things for European research project consortia that wish to process information from user profiles. Moreover, the argumentation of the Article 29 Working Party fails to take into account the practical issue that a user can easily switch between public and private profiles. Can the applicability of the Directive and the relevant national legislation rely on such a “vulnerable” criterion?

### **3.3.2 The applicability of the Data Protection Directive on the processing of pseudonymous data**

The concept of personal data is highly contextual, as personal data is any piece of information that can be linked to a natural person. This issue raises difficulties for research projects that wish to be able to easily classify information as personal data or not and process them accordingly. Especially interesting is the question **whether information relating to avatars and pseudonyms should be considered as personal data**. Only when full anonymisation of personal data can be ensured, their processing does not fall under the Data Protection Directive. However research projects such as +Spaces, that gather social network information for producing **reputation** or for **recommendation** purposes, cannot use anonymisation techniques and rely on anonymous data. They have to use pseudonyms, as they need to log the history of a “user” for producing his/her reputation or relevant recommendations for him/her. On this point the Greek Data Protection Authority (DPA) published an interesting opinion on the COCKPIT (Citizens Collaboration and Co-Creation in Public Service Delivery) project, which is another research project funded by the European Union FP7 ICT for governance and Policy Modelling.<sup>28</sup> COCKPIT is a research project that aims at the deployment of a new government model that empowers internet users in the decision making process of public administration and processes data relating to user opinions on services offered by public administration, as expressed in dedicated websites, in social networking sites or blogs, usually via the use of a pseudonym.

The Greek DPA found that

---

<sup>27</sup> Article 29 Data Protection Working Party, WP 163, Opinion 5/2009 on online social networking, 12.06.2009, pp. 5-6

<sup>28</sup> <http://www.cockpit-project.eu>



*“under specific circumstances (when [pseudonyms] are repeatedly used by the same natural person and his/her activities are being continuously monitored), [pseudonyms] can lead to the revelation of the identity of the person. In this way, the pseudonym, which is used by a data subject to publish his/her personal opinion on various matters on the internet, can be used as a means for identification of this person. In any case, the name of the user may not be a fictitious name, but the real name of the user may result from it. Therefore the processing of personal data that takes place in the European project COCKPIT, falls under the provisions of law 2472/97<sup>29</sup>, as long as it cannot be excluded that from the pseudonym one can unveil the identity of a person, as well as due to the fact that the identity of the user may result directly from his/her username”.*<sup>30</sup>

Following the reasoning of the Greek DPA, the collection and processing of user data in +Spaces, even when they are pseudonymous ones, should fall under the data protection legislation and pseudonyms should be treated as personal data.

### 3.3.3 Definition of applicable national legislation

As described above in section 3.2, the Athens based partner of +Spaces, ATC, was defined as data controller for the processing of personal data of users within the frame of +Spaces. Therefore the Greek data protection law, law 2472/1997, has been the applicable legislation in relation to the processing of personal data in +Spaces. This information is clearly provided to the users in the +Spaces privacy notice, as shown in Figure 3.

PERSONAL DATA PROTECTION The handling and protection of the personal data of the +Spaces platform is governed by the terms hereof and the provisions of Greek, European and international law on the protection of individuals with regard to the processing of personal data, as well as Decisions of the Hellenic Data Protection Authority, as specified in the +Spaces Privacy Notice.
---

Figure 3: Applicable law in the +Spaces privacy notice

The necessary communication with the Greek Data Protection Authority has been realised by the project partners, mainly by ATC and KU Leuven, and the required notification to the Greek DPA has been filed, as it will further described below in section 3.14.

## 3.4 Definition of an appropriate legal basis

### 3.4.1 Consent as the legal basis in +Spaces

The processing of personal data should be based on a legitimate ground, as specified in Article 7 of the Data Protection Directive, and Article 6 of the Greek Data Protection Law. More specifically Article 6 of the Greek Data Protection Law foresees that the processing is

<sup>29</sup> Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (Νόμος 2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ΦΕΚ Α' 50/10.4.1997), unofficial translation in English of the consolidated version of the law is done by the Hellenic DPA and is available online at [http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH\\_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-MARCH08-EN.PDF](http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-MARCH08-EN.PDF).

<sup>30</sup> Greek Data Protection Authority, “protection of personal data in the frame of the European project COCKPIT”, 22.02.2012, Reg.Nr. Γ/ΕΞ/1335/22-02-2012 (in Greek), p. 2.

allowed only when the data subject has given his/her consent. The data subject's consent<sup>31</sup> is defined in the Greek Data Protection Law as "any freely given, explicit and specific indication of will, whereby the data subject expressly and fully cognisant signifies his/her informed agreement to personal data relating to him/her being processed. Such information shall include at least information as to the purpose of processing, the data or data categories being processed, the recipient or categories of recipients of personal data as well as the name, trade name and address of the Controller and his/her representative, if any. Such consent may be revoked at any time without retroactive effect."<sup>32</sup>

Exceptionally, the processing is allowed without the consent of the data subject, under Article 6(2) of the Greek Data Protection Law, when

- the 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.
- the processing is necessary for the compliance with a legal obligation to which the Controller is subject
- the processing is necessary in order to protect the vital interests of the data subject, if s/he is physically or legally incapable of giving his/her consent
- the processing is necessary for the performance of a task carried out in the public interest or a project carried out in the exercise of public function by a public authority or assigned by it to the Controller or a third party to whom such data are communicated
- the processing is absolutely necessary for the purposes of a legitimate interest pursued by the Controller or a third party or third parties to whom the data are communicated and on condition that such a legitimate interest evidently prevails over the rights and interests of the persons to whom the data refer and that their fundamental freedoms are not affected.

A fundamental question that has to be answered in all EU funded projects (including +Spaces) is **on which grounds the processing of personal data will be based**. In any case, even when users make information publicly available, their processing has to be based on one of the grounds mentioned in Article 7 of the Data Protection Directive.

According to the Greek Data Protection Law, the consent of the data subject, **the consent of the end users** in the case of +Spaces, should be the ground that legitimises the processing of personal data.

The Greek Data Protection Authority (DPA) in its opinion on the EU research project COCKPIT took an interesting position on the legitimate ground based on which the processing of personal data could be collected in that project. Before analysing the position of the Greek DPA, it should be however pointed out that the way how personal data are collected in COCKPIT is significantly different from +Spaces. In COCKPIT the personal data are directly

---

<sup>31</sup> The data subject's consent is defined in Article 2(h) of the Data Protection Directive as "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".

<sup>32</sup> Article 2(k) Greek Data Protection Law.

collected from websites, social networks or blogs that are accessible without the use of any password<sup>33</sup>. According to the opinion of the Greek DPA, the processing of personal data can be considered as compatible with Article 5(2) of the Greek Data Protection Law which foresees that the processing is allowed even without the consent of the data subject when it is “absolutely necessary for the purposes of a legitimate interest pursued by the Controller or a third party or third parties to whom the data are communicated and on condition that such a legitimate interest evidently prevails over the rights and interests of the persons to whom the data refer and that their fundamental freedoms are not affected”. The Greek DPA found that in the case of COCKPIT there was a “higher legitimate interest [of the COCKPIT Project] to be informed of the opinion the recipients of this service, while the rights of the data subject are not prevailing because on the one hand they have publicly expressed their opinion and on the other hand the purpose of the processing is identical to the purpose for which the data subject expressed their opinion (improvement of the service).”<sup>34</sup> It is questionable whether this reasoning could also apply to +Spaces, as the personal data of the users are processed for the above specified purposes. Therefore the +Spaces consortium decided to rely the processing of personal data on the consent of the users, even if that added technical implications to the deployment of the prototype and the pilots.

#### **3.4.2 Information to be given to the data subject**

It is often difficult to define when the consent is informed, as required by the very definition of the term: how much information has to be given to make sure that data subjects understand what is being asked of them? Too much information overwhelms the data subject: a balance has to be found between giving too little and too much information. The Greek DPA paid special attention to the fact that the data subjects have to be informed about the collection and the processing of their personal data. The definition of consent in the Greek Data Protection Law specifies the information that has to be provided to the data subject in order for him/her to be properly informed. Thus, the information to be provided to the data subject should include the purpose of the processing, the data or the categories of data, the recipients or the categories of recipients of the data, as well as the name, the eventual company name and the address of the data controller or their representative.

+Spaces has included the information required by the data protection legislation in the privacy notice of +Spaces (see Annex II: Full version of the +Spaces privacy notice”). Moreover, the relevant information is contained in the consent forms that were signed by the data subjects Twitter (Figure 4) and OpenWonderland (Figure 5), as well as in the information banner for Blogger (Figure 6) and for Facebook (Figure 7). The Facebook and the Blogger API did not allow +Spaces to offer users an active consent action, as in the other virtual spaces (e.g., in the form of a checkbox that enables the “send” button). Therefore an information banner providing the users with the relevant information was offered as an alternative. In the context of installation of cookies, the use of information banners has been recognised by the Article 29 Working Party as a valid way in order to obtain consent:

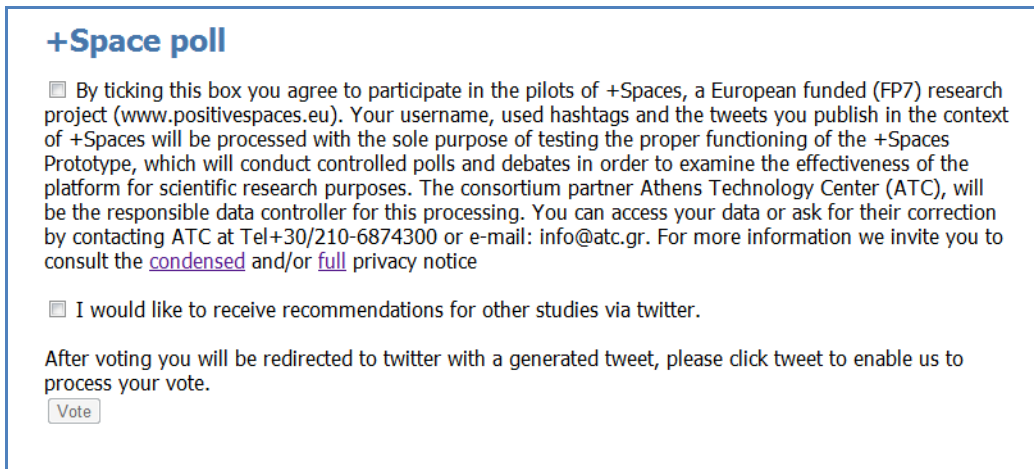
---

<sup>33</sup> Greek Data Protection Authority, “protection of personal data in the frame of the European project COCKPIT”, 22.02.2012, Reg.Nr. Γ/ΕΞ/1335/22-02-2012 (in Greek), p.1.

<sup>34</sup> Greek Data Protection Authority, “protection of personal data in the frame of the European project COCKPIT”, 22.02.2012, Reg.Nr. Γ/ΕΞ/1335/22-02-2012 (in Greek), p. 3.

*“A static information banner on top of a website requesting the user’s consent to set some cookies, with a hyperlink to a privacy statement with a more detailed explanation about the different controllers and the purposes of the processing.”<sup>35</sup>*

Therefore the choice of +Spaces to add an information banner with all the information that had to be provided to the users is fully justified and compliant with the existing legislation.



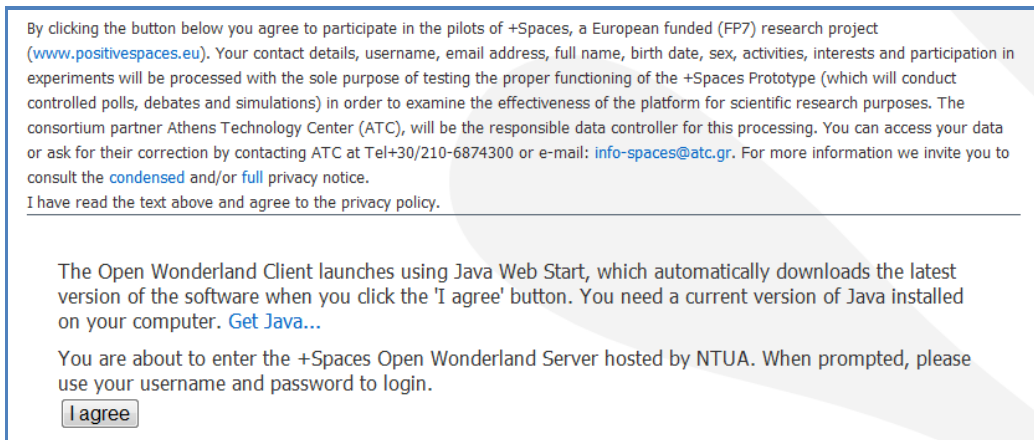
**+Space poll**

By ticking this box you agree to participate in the pilots of +Spaces, a European funded (FP7) research project ([www.positivespaces.eu](http://www.positivespaces.eu)). Your username, used hashtags and the tweets you publish in the context of +Spaces will be processed with the sole purpose of testing the proper functioning of the +Spaces Prototype, which will conduct controlled polls and debates in order to examine the effectiveness of the platform for scientific research purposes. The consortium partner Athens Technology Center (ATC), will be the responsible data controller for this processing. You can access your data or ask for their correction by contacting ATC at Tel+30/210-6874300 or e-mail: [info@atc.gr](mailto:info@atc.gr). For more information we invite you to consult the [condensed](#) and/or [full](#) privacy notice

I would like to receive recommendations for other studies via twitter.

After voting you will be redirected to twitter with a generated tweet, please click tweet to enable us to process your vote.

Figure 4: Consent form in Twitter



By clicking the button below you agree to participate in the pilots of +Spaces, a European funded (FP7) research project ([www.positivespaces.eu](http://www.positivespaces.eu)). Your contact details, username, email address, full name, birth date, sex, activities, interests and participation in experiments will be processed with the sole purpose of testing the proper functioning of the +Spaces Prototype (which will conduct controlled polls, debates and simulations) in order to examine the effectiveness of the platform for scientific research purposes. The consortium partner Athens Technology Center (ATC), will be the responsible data controller for this processing. You can access your data or ask for their correction by contacting ATC at Tel+30/210-6874300 or e-mail: [info-spaces@atc.gr](mailto:info-spaces@atc.gr). For more information we invite you to consult the [condensed](#) and/or [full](#) privacy notice.

I have read the text above and agree to the privacy policy.

---

The Open Wonderland Client launches using Java Web Start, which automatically downloads the latest version of the software when you click the 'I agree' button. You need a current version of Java installed on your computer. [Get Java...](#)

You are about to enter the +Spaces Open Wonderland Server hosted by NTUA. When prompted, please use your username and password to login.

Figure 5: Consent form in OpenWonderland

<sup>35</sup> Article 29 Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, WP188, 08.12.2011.



Figure 6: Information banner in Blogger



Figure 7: Information banner Facebook

### 3.4.3 Some thoughts on the acquisition of user consent in the frame of research projects

The experience of +Spaces showed that **the practice of asking for the consent of the data subjects is very limiting** and actually does not allow the consortia of research projects to fulfil their original plans (to use the “abundance of virtual space users”), as they need to ask consent from each and every user. However, the reliance on another of the grounds specified in Article 7 of the Directive, as for instance claiming that the “processing is necessary for the performance of a task carried out in the public interest”, is difficult to justify under the current legal framework. The establishment of a general exception from the data protection obligations for processing of data that takes place for scientific or research purposes could be proposed as a potential solution. However, such an approach entails the danger that companies and any kind of entities may try to get involved in relevant projects in order to get access to data they wish. In any case, any exception covering the processing for research or scientific purposes would only be relevant for the duration of the research project and wouldn't be enough to justify the processing of data that may continue for the products of the project after it is over. However, the European

Commission, especially in view of the review of the Data Protection Directive, should take into account the problem raised by European research project consortia that the requirement for obtaining user consent, as well as the administrative burden surrounding it (filing notification to the relevant Data Protection Authority/ies, signing of agreements between partners on data protection issues, preparation of consent forms, preparation of privacy notices etc) hinders the conducting of research and the development of innovative and competing tools entailing user data.

### 3.5 Ensuring fairness and transparency of the data processing activities

Article 6 of the Data Protection Directive, as well as Article 4 of the Greek Data Protection Law, lists a series of characteristics that need to be fulfilled in order for personal data to be processed: the data should be processed fairly and lawfully; they should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; they should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; they should be accurate and, where necessary, kept up to date; and they should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. As stressed by BYGRAVE, *'the principles set forth in article 6 of the Directive constitute the essence of the right to data protection. The other provisions of the data protection Directive elaborate on these principles.'*<sup>36</sup>

Fairness is closely linked to the reasonable expectations of the data subject. It refers on the one hand to the fact that *'the collection and further processing of personal data must be carried out in a manner that does not intrude unreasonably upon data subjects' privacy nor interfere unreasonably with their autonomy and integrity. It brings with it the requirements of balance and proportionality. On the other hand, it implies that a person is not unduly pressured into supplying data on himself to a data controller or accepting that the data are used by the latter for particular purposes.'*<sup>37</sup> The requirement of fairness implies that the processing of personal data should be transparent to the data subject.<sup>38</sup> In that sense, recital 38 states that "if the processing of data is fair, the data subject must be in position to learn of the existence of a processing operation and; where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection. This requirement is fulfilled by the information of the data subject." (see section 3.4.2). In the +Spaces project this is achieved through the provision to +Spaces users of clear, complete and accurate information about the data processing activities. More specifically, both a condensed and a full privacy notice have been created by the +Spaces consortium

---

<sup>36</sup> BYGRAVE L. A., *Data Protection Law: approaching its rationale, logic and limits*, Kluwer Law international, 2002, p.43.

<sup>37</sup> BYGRAVE L. A., *Data Protection Law: approaching its rationale, logic and limits*, Kluwer Law international, 2002, p.58.

<sup>38</sup> BYGRAVE L. A., *Data Protection Law: approaching its rationale, logic and limits*, Kluwer Law international, 2002, p.58.

(see Annex II: Full version of the +Spaces privacy notice” and Annex III: +Spaces condensed privacy notice”). Moreover consent forms or relevant information privacy banners were created for all virtual spaces where +Spaces was active (see section 3.4.2).

### 3.6 Definition of the purpose of the processing

Article 6 of the Data Protection Directive, as well as Article 4 of the Greek Data Protection Law mandates that personal data should be collected for specified, explicit and legitimate purposes and they should not be further processed in a way incompatible with those purposes. Defining the purpose of the processing is therefore the first crucial step when assessing the legitimacy of a data processing activity.

The purpose of the processing of user data within +Spaces for the whole duration of the project is limited only to research. Within +Spaces, and as clearly demonstrated in the +Spaces privacy notice, see Figure 8 below, the scientific research purpose is further specified into the three main research goals of the project: (a) the testing of the proper functioning of the +Spaces Prototype and the examination of the effectiveness of the +Spaces platform, (b) the testing of the mechanisms developed in the +Spaces Prototype (e.g. recommendation and reputation systems), and (c) the assessment of the interaction between the users and the application (e.g. role-playing simulation activities, behaviour analysis).

**About the purposes for which your data will be processed.**

Your data that will be collected during the +Spaces Pilots are going to be processed for scientific research purposes and in particular (i) the testing of the proper functioning of the +Spaces Prototype and the examination of the effectiveness of the +Spaces platform and, (ii) the testing of the mechanisms developed in the +SpacesPrototype (e.g. recommendation and reputation systems), (iii) and the assessment of the interaction between the users and the application (e.g. role-playing simulation activities, behaviour analysis).

Your data will not be used for any other purposes than those listed above. Your data will not be used for direct marketing purposes.

Figure 8: Purpose specification in the +Spaces privacy notice

The personal data of the users will not be used by the +Spaces consortium for any other purposes than the aforementioned ones, explicitly described in the privacy policy.

### 3.7 Data minimisation principle

Under Article 6(c) of the Data Protection Directive and Article 4(1)(b) of the Greek Data Protection Law, the data to be processed should be adequate, relevant and not excessive in relation with the purpose of the processing (data minimisation principle). The data minimisation principle acts here as a barrier in order to limit the collection of data which would not be strictly necessary for the provision of the service.

The +Spaces consortium conducted a dedicated analysis of the personal data that would be needed for the project to achieve its purposes, including the demanding reputation and recommendation system. However, it managed to strike a balance between the needs of the application to function in an optimized way and the requirements of collecting only the data strictly necessary for providing the service. The +Spaces consortium made a very careful and detailed analysis of the personal data of users that would be collected in the various virtual

spaces, making substantial differentiations between them. For example, in Twitter the +Spaces system is collecting only the username, the used hashtags and the tweets that users publish in the context of +Spaces. In Blogger, on the other hand, the username, the list of blogs, the used tags and the comments of the users on the +Spaces blog posts are collected and processed. The types of personal data that are processed are clearly depicted in the consent forms and the information banners that were developed for each dedicated space, as shown in figures 4, 5, 6, and 7 above. The +Spaces privacy notice contains an aggregated list of the user data that are processed by the various virtual spaces, as shown in Figure 9.

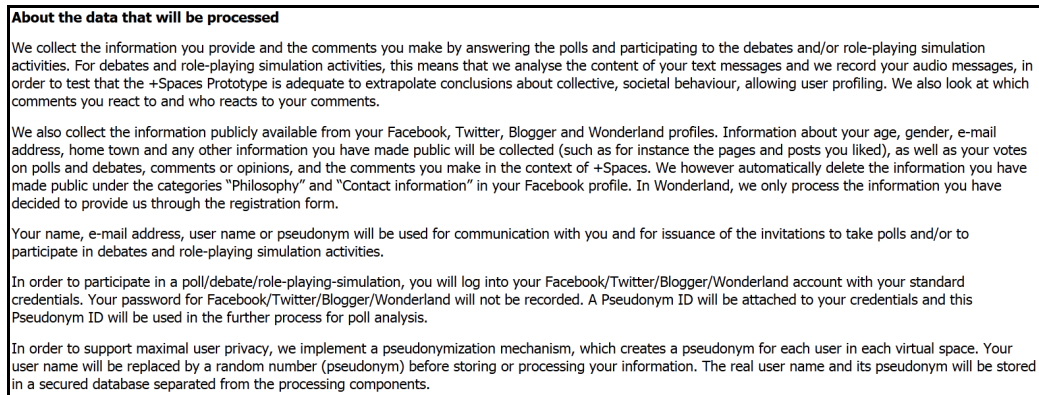


Figure 9: User data to be processed according to the +Spaces privacy notice

### 3.8 Collection of sensitive data

The research projects funded under the Objective ICT 2009-7.3: ICT for governance and Policy Modelling of the 7<sup>th</sup> Framework Programme, as the title of the Objective implies, will often need to process information relating to political opinions of the users. Such data belong to a special category of data, commonly known as **sensitive data**. These data are specified in Article 8 of the Data Protection Directive and are 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. The Greek Data Protection Law defines sensitive data as “data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership to a trade-union, health, social welfare and sexual life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas”<sup>39</sup>. Under Article 8 of the Data Protection Directive, the processing sensitive data is prohibited unless the data controller can rely on one of the grounds listed in Art. 8(2). Sensitive data can be processed when users have given their explicit consent (or their written consent, according to the Greek Data Protection Law) or when these data have manifestly been made public by the data subject. Both grounds are contained into the Greek Data Protection Law (Art. 7(2)(a) and 7(2)(c) respectively).

The purpose of +Spaces is at no case to gather and process users’ sensitive data. In that sense, everything is done as to reduce the possibilities to collect such information. In that

<sup>39</sup> Article 2(b) Greek Data Protection Law.



sense, the questions of the polls were formulated in such a way as to avoid the collection of any sensitive data. However, it is not excluded that sensitive information is gathered when users have made this information public in their profiles of virtual spaces, in which case the prohibition of processing does not apply. The Greek DPA confirmed this approach in its opinion on the COCKPIT project.<sup>40</sup> An additional safeguard that +Spaces took in order to ensure that users were aware of such processing was to include in both the full and the condensed privacy notice a warning about the processing of such information, as shown in Figure 10.

**Sensitive data**  
You should be aware that by participating in the debates or to the role-playing simulation, you may inadvertently reveal information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning your health or your sex life. We ask you to be careful and not to reveal any information you would like to keep confidential. In any case, we will never ask you to provide us with such information, nor will this information be used as criteria for analysis by the data analysis service, the recommendation or the reputation systems or any other service provided by the prototype. However, if you decide to reveal this information while interacting on the +Spaces platform, you expressly consent to have this information processed for the purposes mentioned above in the "Uses" section.

Figure 10: Processing of sensitive data in +Spaces privacy notice

### 3.9 Conservation of the data

In accordance with Article 6(e) of the Data Protection Directive and Article 4(1)(d) of the Greek Data Protection Law, the data should not be stored for a period longer than it is strictly necessary for the purposes for which they were obtained and processed. As shown by the recent controversy between popular search engines and the WP29 about the time of retention of users' search data, such provision may not always be easy to implement. In its Opinion 1/2008 on data protection issues related to search engines, the WP29 stated that "search engine providers must delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times"<sup>41</sup>. In the context of the COCKPIT project the Greek DPA found that the storage of the data only for the period that is absolutely necessary for their analysis in the frame of the project and their deletion after the completion of the content analysis complies with the conservation requirement of the data protection legislation. Similarly, the +Spaces consortium will process the user data only for time that is absolutely necessary for the realisation of its purposes and at the latest upon the end of the project or its eventual extension, approved by the European Commission. After this period the data will be either be anonymised or deleted. This is also reflected in the +Spaces privacy notice, as shown in Figure 11 below.

Your data will be deleted or fully anonymised when the research purpose is completed and at the latest by the end of the +Spaces project, i.e. 30/06/2012 or until later end of the +Spaces project, in case of an extension approved by the European Commission.

Figure 11: Information about the deletion of personal data in the +Spaces privacy notice

<sup>40</sup> Greek Data Protection Authority, "protection of personal data in the frame of the European project COCKPIT", 22.02.2012, Reg.Nr. Γ/ΕΞ/1335/22-02-2012, p. 2 (in Greek).

<sup>41</sup> Article 29 Data protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP148, 4 April 2008.

### 3.10 Ensuring the accuracy of the data

The European, and consequently also the Greek, data protection legislation require that personal data processed are accurate and kept up to date. In order to comply with this principle within the context of +Spaces and as +Spaces did not have any other way to ensure the accuracy of the data, the consortium chose to enable users to ask for the correction of their data. To that effect, users were given an email address, a phone number and a fax number where they could ask for the correction or deletion of inaccurate data. This action on behalf of the data subject, also corresponds to the right of access that the data protection entrusts them with and will be further explained below in section 3.11.

### 3.11 Rights of the data subjects

The data protection legislation ensures some rights to the data subject that have to be safeguarded by the data controller in order to allow them to “participate in, and have a measure of influence over, the processing of data on them by other individuals or organisations”<sup>42</sup>. These rights are the provision of the necessary information that personal data of an individual are being collected and processed, the right of access to the personal data and the right to object to the processing. The data subjects are informed about the processing of their personal data via the presence of consent forms and informational privacy banners, as already described above.

Article 12 of the Data Protection Directive, as well as Article 12 of the Greek Data Protection Law, grants the data subject a right to ask for the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the data protection legislation, in particular because of the incomplete or inaccurate nature of the data.

Pursuant to Article 14(a) of the Data Protection Directive and Article 13 of the Greek Data Protection Law, the data subject should also be granted the right to object, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him. This right is conditioned to the existence of legitimate reasons, unless where the processing satisfies a legal obligation or where an explicit provision of the decision that authorises the processing excludes the application of these provisions. The controller is entitled to evaluate the legitimacy of the request and to deny it. The +Spaces consortium has reserved the right to ask for a legitimate reason, when the request for deletion of data could put in risk the success of on-going test of +Spaces.

Within +Spaces the end users are clearly informed about their aforementioned rights both in the +Spaces privacy notice (see Figure 12) as well as in the dedicated consent forms and information banners in the various virtual spaces.

---

<sup>42</sup> BYGRAVE L. A., *Data Protection Law: approaching its rationale, logic and limits*, Kluwer Law international, 2002, p.63

**About your rights**

You can have access to your personal data and ask for their correction or deletion by contacting the +Spaces Consortium partner Athens Technology Center (ATC) (, Rizariou 10, Chalandri 152 33, Athens, Greece, Tel:+30/210-6874300, Fax: +30/210-6855564, e-mail: info@atc.gr.

To protect your privacy and the privacy of others, we may have to verify that you are who you are before we can give you access to, or change, information about you. If your request for deletion could put at risk the success of the on-going tests, we may ask you to provide a legitimate reason.

Figure 12: Exercise of user's rights in +Spaces privacy notice

### 3.12 Confidentiality of the data

The data controller has to implement security measures sufficient to guarantee the confidentiality of the processing (Article 16 and 17 of the Data Protection Directive; Article 10 of the Greek Data Protection Law). These measures should be both physical and logical and should be adapted to the nature of the data processed and to the risks offered by the processing. Appropriate security measures should 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. This includes the prevention of occurrence such as the dissemination of information that may be helpful to protect a right of the data subject, a third party or the data controller himself – also with a view to preventing manipulation, alteration or destruction of data and related items of evidence. Specific care should be put on the persons entitled to access to the images and to process them, particularly when the controller opts for sub-contracting part or the whole processing to a processor<sup>43</sup>. Any person acting under the authority of the controller or of the processor, including the processor himself who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

When the processing is carried out on the behalf of the controller, the processor should provide sufficient guarantees in respect of the technical security measures and organisational measures and must ensure compliance with those measures. The carrying out of the processing by a processor should be governed by a contract or legal binding act done in a written form. The processor should act only on instructions from the controller.

Deliverable 3.2.4 has addressed the security measures that will be implemented into the +Spaces platform to ensure the confidentiality of the data. Moreover, the issues relating to the security and the confidentiality of the data have been included in the agreements that have been signed between the data controller, ATC, and the data processors, NTUA and Fraunhofer, as indicated in Annex I: Controller/processor agreements". Finally, the end users are informed about the security measures taken within +Spaces in the +Spaces privacy notice, as shown in Figure 13.

---

<sup>43</sup> The processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Article 2 (e) of Directive 95/46/EC).

#### Security measures

Appropriate security policies, rules and technical measures are implemented to protect your personal data that will be revealed via the Prototype and will be stored on the +Spaces Platform from unauthorised access, including use of firewalls where appropriate. All communication is encrypted and the access is strictly restricted for third parties. Requests that do not present the security identity of the sending entity are discarded. Additionally, any direct connections between an external service and the Front End are secured.

All the employees and data processors, who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of the your personal data.

Figure 13: Security measures in the +Spaces privacy notice

### 3.13 International transfers of personal data

The data protection legislation prohibits transfers of personal data to third countries unless these countries provide for an adequate level of protection. In the beginning of the project it was discussed whether personal data of +Spaces users would be sent to Israel (IBM) for analysis. Israel has been acknowledged as providing an adequate level of protection by the Commission Decision 2011/61/EU of 31 January 2011, meaning that no additional safeguards to the ones usually required for transfers of personal data to any other Member States were required<sup>44</sup>. However, the consortium decided to avoid the transfer of personal data outside the European Union and the Data extraction would take place on NTUA servers, based in Athens.

### 3.14 Notification of the processing to the competent Data Protection Authority

When any data processing operation is carried out, the data controller has to notify the respective Data Protection Authority. As the data controller for the +Spaces project was ATC, the respective DPA was the Greek one. In accordance with the notification obligation, as stated in Article 6 of the Greek Data Protection Law, and with the procedure required by the Greek Data Protection Authority, ATC in collaboration with the legal partner of +Spaces, KU Leuven, prepared the necessary documentation and filed duly the notification. The registration number of the notification is: ΓΝ/ΕΙΣ/1200/20-10-2011

## 4 Legal evaluation of +Spaces in Greece

### 4.1 Legislative process in Greece

The legislation initiative lies in the Government, which introduces Bills, and the Parliament, which introduces Law Proposals.

All laws are voted (enacted) in a plenary session. They may be voted by standing parliamentary committees. In case of the latter, the Plenum subsequently meets to have a debate and vote, in one session.

It is mandatory that an explanatory report is attached to Bills and Law Proposals; as such

<sup>44</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:en:PDF>

report elaborates on the purpose of the proposed legislation and indicates the exact wording of current legislation to be amended or repealed. If a Bill or a Law Proposal incurs additional expenses for the State Budget, it then has to be accompanied by a General Accounting Office's report specifying the amount of the expenditure involved. If a Bill results in expenditure or reduction of revenues, a special report regarding the coverage of the expense is attached and it is signed by both the Minister of Finance and the competent Minister. Bills must also be accompanied by an Impact Assessment Report and by a report on the results of the public consultation that took place prior to the submission of the Bill. Furthermore Bills and Law Proposals may be transmitted to the Scientific Agency of the Hellenic Parliament, which submits a review on the proposed provisions.

Amendments and additions to Bills and Law Proposals that are up for voting must be introduced at the latest three days prior to the debate and on Fridays it must take place until 13:00 the latest and may be introduced by Ministers and MPs alike. Amendments submitted by Ministers are also accompanied by a brief Impact Assessment Report.

The elaboration and examination of a Bill or a Law proposal includes two stages that are at least seven (7) days apart. At the first stage a debate in principle and on the articles is conducted and at the second stage a second reading takes place followed by debate and vote by article. During the legislative elaboration of every Bill or Law proposal from the competent standing committee and until the second reading of the relevant articles, every special permanent committee can express its opinion on any specific issue that falls within its competence.

## **4.2 Procedures of Parliamentary Control**

The Plenum exercises parliamentary control at least twice a week including: a) petitions, b) questions, c) current questions, d) applications to submit documents, e) interpellations and f) current interpellations, g) investigation committees.

Documents by means of which Parliamentary control is exercised are submitted to Parliament and ought to mention which Minister they are addressed to. The appropriate Hellenic Parliament Department shall enter them by date (in chronological order) to special volumes, one for each different category, numbering them in continuous sequence. The Minister receives a copy of the document submitted, i.e. of the parliamentary control medium used. Parliamentary control means and written responses to such means may be also come in electronic format.

At the same time a copy of the transmitted document is forwarded to the relevant agency of the parliament and to the MP who initially exercised parliamentary control. In this case the deadline for a reply starts five days posterior to the date of the forwarded document.

Parliamentary control means shall be processed within the regular session they were presented. Should parliamentary control means not have been debated until the end of the regular session, they may be submitted anew in which case their sequence number in the respective archives is determined by the order in which they were submitted.

Lists and tables on relevant documents for exercising parliamentary control are forwarded to MPs regularly.

To assist the Plenum or the Recess Section with their parliamentary control workload, standing committees also exercise capacities as specified in the Standing Orders.

### 4.3 Interesting Means of Parliamentary Control

Parliamentary control means, other than a censure motion (art. 142) include: a) petitions, b) questions, c) current questions, d) applications to submit documents, e) interpellations and f) current interpellations, g) investigation committees.

#### A) Petitions

Individuals or groups of citizens may address Parliament in writing to make complaints or requests. Parliamentarians may endorse such petitions. A Minister should reply within 25 days to a petition endorsed by an MP.

#### B) Questions

Parliamentarians have the right to submit written questions to Ministers regarding any matter of public importance. Such questions aim at keeping the Parliament updated on specific issues. Ministers must reply in writing within twenty five days. In any case, at the start of the week in session such questions are on the agenda and questions as well as petitions are discussed.

#### C) Current questions

Every Parliamentarian has the right to raise an issue of current significance and address a question to the Prime Minister or the Ministers which for their part should give an oral response to. Once a week, at least, the Prime Minister selects 2 questions to be answered. Current questions are debated in the Plenum, thrice weekly, as well as in the Recess Section.

#### D) Applications to Submit Documents

Parliamentarians have the right to request from Ministers in writing, to supply documents related to issues of public importance. The Minister has one month at his/her disposal to submit the documents requested. Still, no documents relating to diplomatic, military or pertinent to national security issues may be submitted.

#### E) Interpellations

Interpellations aim at the control of Government for actions or omissions. MPs that have submitted questions or applied for the supply of specific documents, may turn them into interpellations should they deem that the minister's response did not suffice. Interpellations are debated in Plenary Sessions. Should there be more than one interpellation about the same subject the Parliament may decide on their simultaneous debate or even proceed into a general discussion.

#### F) Current Interpellations

Parliamentarians have the right to current interpellations on current affairs. Such interpellations may be debated on Mondays in Plenary Sessions as well as in specified sittings of the Recess Section. As a general rule, the same debate process for interpellations, as specified by the Standing Orders, also applies in the case of discussing current interpellations.

### 4.4 Possible Use of +Spaces tools in the legislative procedure

+Spaces tools could be used in selective sub-stages of the legislative procedure as presented above. In the next table +Spaces tools are correlated with most of the steps of a formal legislative procedure. The added value of +Spaces tools is also presented.

+Spaces tools as presented more explicitly in the other project deliverables could be used in selective sub-stages of the legislative procedure as presented above in the Hellenic Parliament legislation procedures workflow. +Spaces tools could be summarized to the following:

+Spaces polls in Twitter and Facebook

+Spaces debates in Facebook and Blogger

+Spaces role playing simulations in Twitter and Open Wonderland

All the above-mentioned tools are fully integrated and interoperable using a set of services like Data Analysis Service and Reputation Service, giving the possibility to the policy makers to easily understand in a visual and user friendly environment the citizens responses, reactions, comments, suggestions, ideas and of course an initial societal impact analysis of the policy measures adopted by them.

In the next table all +Spaces tools are correlated with each steps of a formal legislative procedure. The added value of +Spaces tools is also presented, as well as the policy making actors involved for the legislation formation, debate and final release. Additionally another step of the formal legislation procedure was added, the Parliamentary Control *“called Ex-Post legal evaluation”* where +Spaces tools are also play a significant role.

It is evident that all +Spaces, tools, services, capabilities are fitting to several steps of the formal legislative procedure followed in the Hellenic Parliament. Please note that the legislative steps already presented above are the formal steps of the legislative democratic procedure of any Parliament.

	<b>Legislative Procedures</b>	<b>+Spaces Tool</b>	<b>Added Value</b>
1	Legislation Draft Formation	Polls	Citizens primary reactions
2	E-consultation	Polls & Debates	Comments, Reactions, Suggestions from citizens
3	Draft Legal Element Submission		
4	HeP Committees Discussions	Polls & Debates with Role Playing	Live Debates with citizens and groups of interest
5	Plenary Debates for Legal Element Approval	Polls, Debates, Role Playing output	Concrete Report for the Plenary
6	Legal Element integration into existing legislation		
7	Parliamentary Control (Ex-Post legal evaluation)	Polls & Debates & Role Playing	Comments, Impacts, Reactions, New Ideas, Complaints, Suggestions from citizens

## 5 Conclusions

+Spaces has been a very interesting project for the carrying out of legal research. The legal research focused on two main areas. On the one hand it analysed the Terms and Conditions of virtual spaces relevant to the +Spaces project, i.e. Facebook, Twitter, Blogger and OpenWonderland and it spotted the impact of some of the terms on the development of the +Spaces prototype and its functionalities. On the other hand, and due to the fact that the +Spaces pilots were making use of user data, albeit pseudonymised, the research focused mainly on the protection of personal data.

The +Spaces consortium organized two workshops related to legal issues, led by the legal partner, KU Leuven, organised two workshops relating to legal issues. The first +Spaces Workshop on the Privacy and Data Protection Framework was organised in December 2010, with the participation of the European research projects that were funded under the same objective. KU Leuven gave an overview of the data protection framework that had to be taken into account by the various consortia, highlighting however that a number of data protection issues in virtual spaces were still open for research. The second +Spaces workshop on “Legal challenges for FP7 projects” was organised in collaboration with the WeGov project as part of the Samos Summit 2012. The workshop aimed at presenting issues, challenges and possible difficulties that EU research projects deal with, focusing mainly on the ones relating to legal and ethical ones. The +Spaces partner, KU Leuven, gave a presentation on “Legal Issues while researching users' behaviour in virtual spaces” presenting the +Spaces experiences in relation to legal issues.

The legal partner of the consortium, KU Leuven, dedicated a large amount of its time and resources in order to carry out the two main tasks described above, the analysis of the Terms and Conditions and the specification of the data protection related requirements striving at ensuring that the privacy of the users is protected and that the +Spaces platform as well as the respective pilots are legally compliant. In practice, currently the legal partners participating in European research projects focus on ensuring that the processing of personal data is compliant with the current European legal framework. To this end, they have to inform the relevant national Data Protection Authorities and they will cooperate with them for resolving any eventual issues. However, this should not be the main task of a



research partner and the European Commission should try to find alternative ways in order to allow legal partners to focus on fundamental research instead of focusing on compliance issues. Therefore the European Commission considers the simplification the procedures relating to the processing of personal data for research purposes. It is positive to see that the European Commission has spotted this issue, and it seems that in order for new European projects to be funded, there needs to be a clear agreement on the role of the various partners in relation to the processing of personal data of individuals.

## 6 Annex I: Controller/processor agreements

### A. Controller/Processor Agreement between ATC and Fraunhofer

#### Controller-Processor Agreement

Between :

Athens Technology Center S.A. (ATC), located at Rizariou 10, Chalandri 152 33, Athens, Greece, duly represented by Dr. Andreas Kalligeris Skentzos (Director) and Nikolaos Tsaourakis (CEO)

Hereinafter : Controller

And :

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastrasse 27c, 80686 Munich for its Fraunhofer Institute for Algorithms and Scientific Computing SCAI, located at Schloss Birlinghoven, 53754 Sankt Augustin, Germany, duly represented by Professor Dr. Martin Hofmann-Apitius, Head of Department of Bioinformatics

Hereinafter : Processor

Preamble:

WHEREAS, the Parties are research partners in the +SPACES (Policy Simulation in Virtual Spaces) project (hereinafter: Project), a Specific Targeted Research (STREP) supported and funded by the European Union under the 7th Framework Programme for Research and Technological Development within the ICT for Governance and Policy Modelling (ICT-2009.7.3).

WHEREAS, one of the Project results is the development and realization of the +SPACES Prototype, a tool allowing the exploitation of virtual worlds as knowledge containers for assessing public reaction which will be supported by a service oriented platform and will allow added value services to be incorporated.

WHEREAS, the functioning of the Prototype and related tools shall be tested within a demonstrator field test (hereinafter: Pilot) in virtual worlds as described and planned in the work plan in the Description of Work (Annex I to the Grant Agreement no. 248726 for the Project ).

WHEREAS, in order to ensure the protection and security of data collected during the Pilot and being passed from the Controller to the Processor, the Parties agree to conclude the following agreement:

#### **Article 1 – Definitions**

- 1.1 'Controller' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: Directive 95/46/EC), i.e. "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.
- 1.2 'Data' shall mean any information collected on and extracted from the +Spaces platform during the Pilot
- 1.3 'Personal Data' shall have the same meaning as in Directive 95/46/EC, i.e. "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";
- 1.4 'Processor' shall mean a natural or legal person, public authority, agency or any other body which processes Data provided or made accessible by the Controller on behalf of the Controller"
- 1.5 'Pseudonymised Data' shall mean any Data in which personal identifiers have been removed and been replaced by an artificially-created identifier / code so as to conceal the identity of the person the Data was originally related to.
- 1.6 'Processing Services' shall mean the processing of Pseudonymised Data by the Processor by performing statistical or other analysis of aggregated Pseudonymised Data on the authorization or behalf of the controller in relation to the Pilot and in accordance with the instructions of the Controller and in compliance with the applicable data protection laws.

#### **Article 2 - Subject**

- 2.1 This agreement shall apply to Data which has been pseudonymised by the Controller (Pseudonymised Data) and which is being
  - a) sent from the date of this agreement by the Controller to the Processor for processing,

- b) accessed by the Processor on the authority of the Controller for processing from the date of this agreement, or
  - c) otherwise received by the Processor for processing on the Controller's behalf
- 2.2 The Parties agree that the Controller shall not provide or grant access to any Data which has not been pseudonymised so to prevent that the Processor will receive or get access to any Personal Data. Furthermore, it is agreed that the links between the artificial and normal identifiers (or the cipher) are stored separately and securely by the Controller.
- 2.3 The Processing Services are executed on behalf of the Controller and in compliance with his instructions as specified and agreed for the Pilot in the project documents. All instructions and specifications, if in writing, will be included as addenda in this agreement with specific reference to the date of their issuing.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1 The Controller represents and warrants that he has instructed and throughout the duration of the Processing Services will instruct the Processor to process the Pseudonymised Data only on the Controller's behalf and in accordance with the applicable data protection laws.
- 3.2 The Controller will instruct the Processor on the technical and organizational security measures, to be implemented by the Processor, according to the progress realised by the +SPACES consortium on these issues.
- 3.3 The Controller agrees that he shall ensure that he complies at all times with the applicable data protection laws, in particular Directive 95/46/EC and any national laws applicable.
- 3.4 The Controller represents and warrants that any and all Data which is sent or made accessible to the Processor has been pseudonymised and does not include any Personal Data so to protect the Personal Data collected and possessed by the Controller against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.
- 3.5 The Controller warrants that any documents used for the pseudonymisation of the Data, in particular those containing the links between the artificial and normal identifiers (or the cipher), will be stored separately and securely by Controller and will not be made accessible to the Processor in any way.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he has followed and throughout the duration of the Processing Services will follow the instructions of the Controller to process the Pseudonymised Data. The Processor will process the Pseudonymised Data only in the manner permitted by the Controller. The Processor will receive from the Controller only

Pseudonymised Data. The Processor agrees that all relevant and required logs will be kept at least for the duration of the Project.

4.2. The Processor further agrees that he shall not apply or use the Pseudonymised Data for purposes other than specified in this Agreement and shall not communicate the Pseudonymised Data to third parties. Such communication will not take place even for preservation purposes. The Processor shall at all times keep the Pseudonymised Data confidential and request its employees to keep the Pseudonymised Data confidential as well.

4.3. The Processor undertakes and warrants that he will implement the technical and organizational security measures before the start of processing the Pseudonymised Data and warrants to take all necessary data security measures.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to his processing of the Pseudonymised Data for the Pilot and to abide by the advice of the supervisory authority, as defined in the relevant legislation or regulations, with regard to the processing of this Pseudonymised Data.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Pseudonymised Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access by third parties, and (3) any request received from the data subjects.

4.6. The Processor agrees and undertakes to assist the Controller in his obligation to grant the right of information, rectification and erasure.

4.7. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

## **Article 5 – Term and Termination**

This Agreement enters into force on the date of the last signature.

It shall terminate automatically upon termination or expiry of the Processor's obligations in relation to Processing Services, however, no later than 30.06.2012.

Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.

The Parties agree that upon termination of this Agreement, the Processor shall, at the choice of the Controller, transmit and/or return all the Pseudonymised Data in his possession or under his control along with all copies, support and documentation containing Pseudonymised Data received from the Controller and processed thereof or shall destroy all the Pseudonymised Data and certify to the Controller that he has done so, unless legislation

imposed upon the Processor prevents him from returning or destroying such Pseudonymised Data. In that case, the Processor warrants that he will guarantee the confidentiality of the Pseudonymised Data and will not process the Pseudonymised Data anymore unless required by the law or instructed by the Controller.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of Greece shall apply to this Agreement.  
In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled in due time, either party may bring the dispute to a competent court in Athens, Greece

**Article 7 Final clauses**

- 7.1 Should a provision of this agreement be invalid or become invalid or should this agreement contain an omission, then the legal effect of the other provisions shall not thereby be affected. Instead of the invalid provision a valid provision is deemed to have been agreed upon which comes closest to what the parties intended commercially; the same applies in the case of an omission.
- 7.2 This contract shall not be modified or changed except in writing; this shall also apply to any waiver of this requirement. Changes and amendments must be identified as such.

Done in in two copies, each party having received one.

Athens, (date)

ATC

-----

Dr. Andreas Kalligeris Skentzos  
Director

-----

Nikolaos Tsabourakis  
CEO

Sankt Augustin, (date)

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.

-----

-----

Prof. Dr. Martin Hofmann-Apitius  
Head of Department of Bioinformatics

Klarissa Al-Shorachi  
Legal Affairs and Contracts

## **B.Controller-Processor Agreement between ATC and NTUA**

### Controller-Processor Agreement

Between:

Athens Technology Center S.A. (ATC), located at Rizariou 10, Chalandri 152 33, Athens, Greece, duly represented by Dr. Andreas Kalligeris Skentzos (Director) and Nikolaos Tsaourakis (CEO)

Hereinafter: Controller

And:

ICCS/NTUA, Zografou Campus, Heroon Polytechniou 9, 15780, Zografou, Athens, Greece, duly represented by Prof. Yiannis Vassiliou (Director).

Hereinafter: Processor

WHEREAS, the Parties are research partners in the +SPACES (Policy Simulation in Virtual Spaces) project, a Specific Targeted Research (STREP) supported by the European Union under the 7th Framework Programme for Research and Technological Development within the ICT for Governance and Policy Modelling (ICT-2009.7.3).

WHEREAS, one of the Project results is the development and realization of the +SPACES Prototype, a tool allowing the exploitation of virtual worlds as knowledge containers for assessing public reaction which will be supported by a service oriented platform and will allow added value services to be incorporated.

WHEREAS, the functioning of the Prototype and related tools shall be tested within a demonstrator field test (hereinafter: Pilot) in virtual worlds as described and planned in the work plan in the Description of Work (Annex I to the Grant Agreement no. 248726 for the Project ).

WHEREAS, the Pilots are foreseen in the +SPACES Description of Work (Annex I to the Grant Agreement no. 248726 for the Project). It is planned in +SPACES Deliverable 6.1 "Pilot Scenarios", which was submitted to the European Commission on 30.05.2011, and the details thereof are further described in the +SPACES workplan (workplan is described in Description of Work, Annex I to the Grant Agreement no. 248726 for the Project).

WHEREAS, ATC will take the responsibility for the pilots, in particular the acquisition, the management and processing of certain personal data, which are produced during the pilots,



within the scope of the +Spaces Deliverable 6.1 “Pilot Scenarios” for the above mentioned testing purposes, as the Controller of the personal data.

WHEREAS, the Processor, ICCS/NTUA, agrees to host the servers where the data collected during the pilots will be stored and to collect, to process and/or to receive personal data on behalf of the controller for the above testing purposes as specified in the workplan found in Description of Work, in accordance with the instructions of the controller and in compliance with the applicable data protection laws.

WHEREAS, in order to ensure the protection and security of data collected during the Pilots and being passed from the Controller to the Processor, the Parties agree to conclude the following agreement:

#### **Article 1 – Definitions**

1.1. ‘the Controller’ shall have the same meaning as in Directive 95/46/EC i.e. 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;

1.2. ‘the Processor’ shall have the same meaning as in Directive 95/46/EC and means the entity who agrees to collect, to process or to receive personal data in relation with the field test, and intended for processing on behalf of the Controller in accordance with his instructions, the terms of this Agreement and the applicable data protection laws;

1.3. ‘Data’ shall mean any information collected on and extracted from the +Spaces platform;

1.4. ‘Personal Data’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC), i.e. “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”;

1.5. ‘Pseudonymised Data’ shall mean any Data in which personal identifiers have been removed and replaced by an artificially-created identifier / code so as to conceal the identity of the person the Data was originally related to;

1.6. ‘Pilot’ shall mean the demonstrator field test as described and planned for +SPACES deliverable 6.1 “Pilot Scenarios”, which was submitted to the European Commission on 30.05.2011.

#### **Article 2 - Subject**

2.1 The Controller requests the Processor, who accepts and agrees, to host on its servers and to process on his behalf and in compliance with his instructions Pseudonymised Personal Data as specified and agreed for the Pilots.

2.2 Parties agree that the specifications and the instructions for the processing of the Pseudonymised Personal Data for the testing purposes of the Pilots are further described in the internal project documents and additional documentation that parties may agree upon from time to time. All instructions and specifications, if in writing, will be included as addenda in this agreement with specific reference to the date of their issuing.

### **Article 3 – Warranties and obligations of the Controller**

3.1. The Controller agrees and warrants that he has instructed and will instruct throughout the duration of the Pseudonymised Personal Data processing services the Processor to process the Pseudonymised Personal Data only on the Controller's behalf and in accordance with the applicable data protection laws.

3.2. The Controller will instruct the Processor on the technical and organizational security measures, to be implemented by the Processor, according to the progress realised by the +SPACES consortium on these issues. Parties agree and believe that to the best of their knowledge these measures are adequate to protect the Pseudonymised Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, having regard to the state of the art and the cost of their implementation.

### **Article 4 – Warranties and obligations of the Processor**

4.1. The Processor agrees and warrants that he has followed and will follow throughout the duration of the Pseudonymised Personal Data processing services the instructions of the Controller to process the Pseudonymised Personal Data and will process the Pseudonymised Personal Data only on the Controller's behalf and in accordance with the applicable data protection laws. The Processor will process the data only in the manner permitted to the Controller himself. The Processor agrees that he shall render the Pseudonymised Personal Data anonymous as soon as the scientific research purpose permits it.

4.2. The Processor further agrees that he shall not apply or use the Pseudonymised Personal Data for purposes other than specified in this Agreement and shall not communicate the Pseudonymised Personal Data to third parties, even not for their preservation. The Processor shall at all times keep the Pseudonymised Personal Data confidential and requests its agents to keep the Pseudonymised Personal Data confidential as well.

4.3. The Processor undertakes and warrants that he will implement the technical and organizational security measures before the start of processing the Pseudonymised Personal Data and guarantees to take all the agreed data security measures in accordance with the Deliverable 6.1 "Pilot Scenarios", which was submitted to the European Commission on 30.05.2011.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to his processing of the Pseudonymised Personal Data for the Pilots and to abide by the advice of the supervisory authority as defined in the relevant legislation or regulations with regard to the processing of this Pseudonymised Personal Data.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Pseudonymised Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access by third parties, and (3) any request received from the data subjects.

4.6. The Processor agrees and undertakes to create assist the controller in his obligation to grant the right of information, rectification and erasure.

4.7. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

#### **Article 5 – Term and Termination**

The Agreement is concluded for the period and the time required for the testing of +SPACES Prototype in the framework of +SPACES Pilots. The agreement ends latest upon the end of the +Spaces project, at 30.06.2012 or upon the later end of the +Spaces project, in case of an extension approved by the European Commission.

Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.

Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Pseudonymised Personal Data collected and/or processed for the pilots and all the copies, support and documentation containing Pseudonymised Personal Data processed thereof or shall destroy all the Pseudonymised Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Pseudonymised Personal Data and will not actively process the Pseudonymised Personal Data anymore, unless required by the law or instructed by the Controller.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Greece, where the Controller is established, shall apply to this Agreement.

In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled in due time, either party may bring the dispute to a competent court in Greece.

Done in in two copies, each party having received one.

Athens, (date)

ATC

-----

Dr. Andreas Kalligeris Skentzos  
Director

-----

Nikolaos Tsabourakis  
CEO

ICCS/NTUA

-----

Prof. Y. Vassiliou

Director

-----

## 7 Annex II: Full version of the +Spaces privacy notice

### Full version of the +Spaces Privacy Notice

#### User Consent form

#### **Information about the +Spaces Prototype Tests and the processing of your personal data**

The purpose of this form is to inform you of the details of the +Spaces Pilot tests via Facebook and/or Twitter and/or Blogger and/or Wonderland platforms.

You are fully free to participate in the pilots. However, you should only tick the box if you agree with the hereby presented conditions. By ticking the 'I agree' box (for Facebook and Twitter polls), by posting a comment on the Blogger Debate Blog or the Facebook Debate, or by pressing the 'I agree' button in Wonderland you provide your consent to the processing of your personal data as outlined in this notice.

#### **About the +Spaces Prototype.**

The +Spaces Prototype (hereafter "the Prototype") has been developed by the +Spaces Consortium, which is a European funded (FP7) research project (Grant Agreement n°248726).

The Prototype is a tool that allows the deployment of applications in virtual worlds and social networks to stimulate, monitor, link and aggregate user activity so as to test that the +Spaces Prototype is adequate to extrapolate conclusions about collective, societal behaviour, allowing user profiling. More particularly, the prototype enables third parties such as policy makers to gather public's opinion on specific policy issues. The prototype will be tested in +Spaces pilots.

#### **About the organization responsible for the organization of the +Spaces pilot ('data controller')**

+Spaces Consortium partner Athens Technology Center (ATC) (Rizariou 10, Chalandri 152 33, Athens, Greece, Tel+30/210-6874300, Fax: +30/210-6855564, e-mail: info-spaces@atc.gr , is the responsible for the organization of the +Spaces Pilots.

#### **About the purposes for which your data will be processed.**

Your data that will be collected during the +Spaces Pilots are going to be processed for scientific research purposes and in particular (i) the testing of the proper functioning of the +Spaces Prototype and the examination of the effectiveness of the +Spaces platform and, (ii) the testing of the mechanisms developed in the +SpacesPrototype (e.g. recommendation and reputation systems), (iii) and the assessment of the interaction between the users and the application (e.g. role-playing simulation activities, behaviour analysis).

Your data will not be used for any other purposes than those listed above. Your data will not be used for direct marketing purposes.

Your data will be deleted or fully anonymised when the research purpose is completed and at the latest by the end of the +Spaces project, i.e. 30/06/2012 or until later end of the +Spaces project, in case of an extension approved by the European Commission.

#### **About the data that will be processed**

We collect the information you provide and the comments you make by answering the polls and participating to the debates and/or role-playing simulation activities. For debates and role-playing simulation activities, this means that we analyse the content of your text messages and we record your audio messages, in order to test that the +Spaces Prototype is adequate to extrapolate conclusions about collective, societal behaviour, allowing user profiling. We also look at which comments you react to and who reacts to your comments.

We also collect the information publicly available from your Facebook, Twitter, Blogger and Wonderland profiles. Information about your age, gender, e-mail address, home town and any other information you have made public will be collected (such as for instance the pages and posts you liked), as well as your votes on polls and debates, comments or opinions, and the comments you make in the context of +Spaces. We however automatically delete the information you have made public under the categories "Philosophy" and "Contact information" in your Facebook profile. In Wonderland, we only process the information you have decided to provide us through the registration form.

Your name, e-mail address, user name or pseudonym will be used for communication with you and for issuance of the invitations to take polls and/or to participate in debates and role-playing simulation activities.

In order to participate in a poll/debate/role-playing-simulation, you will log into your Facebook/Twitter/Blogger/Wonderland account with your standard credentials. Your password for Facebook/Twitter/Blogger/Wonderland will not be recorded. A Pseudonym ID will be attached to your credentials and this Pseudonym ID will be used in the further process for poll analysis.

In order to support maximal user privacy, we implement a pseudonymization mechanism, which creates a pseudonym for each user in each virtual space. Your user name will be replaced by a random number (pseudonym) before storing or processing your information. The real user name and its pseudonym will be stored in a secured database separated from the processing components.

#### **Sensitive data**

You should be aware that by participating in the debates or to the role-playing simulation, you may inadvertently reveal information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning your health or your sex life. We ask you to be careful and not to reveal any information you would like to keep confidential. In any case, we will never ask you to provide us with such information, nor will this information be used as criteria for analysis by the data analysis service, the recommendation or the reputation systems or any other service provided by the prototype. However, if you decide to reveal this information while interacting on the +Spaces platform, you expressly consent to have this information processed for the purposes mentioned above in the "Uses" section.

#### **About your rights**

You can have access to your personal data and ask for their correction or deletion by contacting the +Spaces Consortium partner Athens Technology Center (ATC) (, Rizariou 10, Chalandri 152 33, Athens, Greece, Tel+30/210-6874300, Fax: +30/210-6855564, e-mail:info@atc.gr.

To protect your privacy and the privacy of others, we may have to verify that you are who you are before we can give you access to, or change, information about you. If your request for deletion could put at risk the success of the on-going tests, we may ask you to provide a legitimate reason.

#### **About the categories of recipients**

##### ***State institutions***

We ensure that your personal data will not be disclosed to State institutions and authorities except if required by law or other regulation.

##### ***Organization analysing poll/debates/role-playing-simulation answers***

The analysis of the poll/debate/role-playing-simulations (text and audio data) will be performed by the Fraunhofer's Data Analysis Service, located at SchlossBirlinghoven, 53754 Sankt Augustin, Germany. The data will first be pseudonymised before they are sent to Fraunhofer's Data Analysis service. The Fraunhofer's Data Analysis Service will be acting as data processor and will process information on behalf and upon further instructions of the data controller ATC.

##### ***Recommendation and reputation systems***

The testing of the recommendation and the reputation services, as well as the processing of related data, will be performed by the National Technical University of Athens, Institute of Communication and Computer Systems (ICCS), located at Zografou Campus, HeroonPolytechniou 9, 15780, Zografou, Athens, Greece . NTUA/ICCS will be acting as data processor and will process information on behalf and upon further instructions of the data controller ATC.

##### ***Hosting***

The servers will be hosted by NTUA, located at Zografou Campus, Heroon Polytechniou 9, 15780, Zografou, Athens, Greece. NTUA will be acting as data processor and will process information on behalf and upon further instructions of the data controller ATC.

##### ***End users***

The activities performed on the platforms (polls/debates/role-play) are performed on behalf of third parties (end users) interested in gathering public opinion about specific policy issues. The data gathered on the +Spaces prototype are pseudonymised before they are shared with these end-users.

#### **Security measures**

Appropriate security policies, rules and technical measures are implemented to protect your personal data that will be revealed via the Prototype and will be stored on the +Spaces Platform from unauthorised access, including use of firewalls where appropriate. All communication is encrypted and the access is strictly restricted for third parties. Requests

that do not present the security identity of the sending entity are discarded. Additionally, any direct connections between an external service and the Front End are secured.

All the employees and data processors, who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of the your personal data.



## 8 Annex III: +Spaces condensed privacy notice

### Condensed notice

The full privacy notice is available [here](#).

#### Scope

- This condensed privacy notice applies to the +Spaces Prototype.

#### Personal Information collected

- We collect information you provide by participating in the polls, debates and role-playing simulation activities.
- We also collect the public information available on your Facebook/Twitter/Blogger/Wonderland profile such as your name, last name, user name, e-mail address, age, gender, and home town. We never collect the information you have made public under the categories “Philosophy” and “Contact information” on your Facebook profile.
- In order to support maximal user privacy, we implement a pseudonymisation mechanism, which creates a pseudonym for each user in each virtual space. Your user name will be replaced by a random number (pseudonym) before storing or processing your information. The real user name and its pseudonym will be stored in a secured database separated from the processing components.
- We keep information on your activity with us and on your interactions with other users.

#### Uses

- We use these data for scientific research purposes in order to examine the effectiveness of the +Spaces platform and to test the proper functioning of the +Spaces Prototype. This prototype is a tool that stimulates, monitors and aggregates user activity so as to assess the potential impact certain policies might have if adopted.
- We process the information we collect about you for exploiting the results from the polls, debates and role-playing simulation activities, after assigning you with a pseudonym. The data are pseudonymised before they are shared with policy makers.
- We process the social information we have about you in order to assess your reputation on the platform and to issue customised recommendations – we may recommend additional +Spaces experiments that may be of interest to you based on your past participation in +Spaces.
- We process the information we collect about you to detect malicious behaviours.
- Your name, last name, user name, e-mail address or pseudonym will be used for

communication with you and for issuance of the invitations for the next trials.

### Choices

- You may access personal information that we hold about you. You can ask us to correct any errors or delete the information we have about you (see below under 'how to contact us' for contact details).
- You may choose not to receive any further contact from us (opt-out).
- To protect your privacy and the privacy of others, we may have to verify that you are who you say you are before we can give you access to, or change, information about you.
- To ensure the reliability of the tests we can ask you to provide a legitimate reason if you require your data to be deleted.

### Important information

- If you do not wish to share some of the information contained in your public profile with us, you should inform us and we will delete this information from our databases.
- Your participation to debates and role-playing simulation activities may in some cases reveal information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. +Spaces consortium will not seek to obtain such information nor will it carry any data analysis based on this information. However, if you decide to reveal this information while interacting on the +Spaces platform, you expressly and explicitly consent to have this information processed for the purposes mentioned above in the "Uses" section.

### How to contact us?

- You can contact +Spaces Consortium partner Athens Technology Center (ATC), via mail: Rizariou 10, Chalandri 152 33, Athens, Greece, via telephone: +30/210-6874300 , via fax: +30/210-6855564, or via e-mail: info-spaces@atc.gr .

## 9 Annex IV: +Spaces Terms of Use

### Terms of Use of the +Spaces Platform

28.03.2012

#### AGREEMENT BETWEEN USER AND +Spaces

The +Spaces Platform is comprised of various Web pages operated by +Spaces.

The +Spaces Web Site is offered to you conditioned on your acceptance without modification of the terms, conditions, and notices contained herein. Your use of the +Spaces Web Site constitutes your agreement to all such terms, conditions, and notices.

#### MODIFICATION OF THESE TERMS OF USE

Positive Spaces reserves the right to change the terms, conditions, and notices under which the +Spaces Web Site is offered, including but not limited to the charges associated with the use of the +Spaces Web Site.

#### LINKS TO THIRD PARTY SITES

The +Spaces Web Site may contain links to other Web Sites (“Linked Sites”). The Linked Sites are not under the control of + Spaces and +Spaces is not responsible for the contents of any Linked Site, including without limitation any link contained in a Linked Site, or any changes or updates to a Linked Site. +Spaces is not responsible for webcasting or any other form of transmission received from any Linked Site. +Spaces is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement by +Spaces of the site or any association with its operators.

#### NO UNLAWFUL OR PROHIBITED USE

As a condition of your use of the +Spaces Web Site, you warrant to +Spaces that you will not use the +Spaces Web Site for any purpose that is unlawful or prohibited by these terms, conditions, and notices. You may not use the +Spaces Web Site in any manner which could damage, disable, overburden, or impair the +Spaces Web Site or interfere with any other party's use and enjoyment of the +Spaces Web Site. You may not obtain or attempt to obtain any materials or information through any means not intentionally made available or provided for through the +Spaces Web Sites.

#### PERSONAL DATA PROTECTION

The handling and protection of the personal data of the +Spaces platform is governed by the terms hereof and the provisions of Greek, European and international law on the protection of individuals with regard to the processing of personal data, as well as Decisions of the Hellenic Data Protection Authority, as specified in the +Spaces Privacy Notice.

#### TERMS OF SERVICE OF OTHER WEBSITES

In order to participate in a poll/debate/role-playing-simulation, you will log into your Facebook/Twitter/Blogger/Wonderland account with your standard credentials. We assume that you have read and understood the Terms of Service, as well as the privacy policies of these websites (Facebook, Twitter, Blogger or Wonderland) and that you agree therewith when you are participating in the +Spaces pilot.

#### PROPER USE OF COMMUNICATION SERVICES

The +Spaces Web Site may contain bulletin board services, chat areas, news groups, forums, communities, personal web pages, calendars, and/or other message or communication facilities designed to enable you to communicate with the public at large or with a group (collectively, "Communication Services"), you agree to use the Communication Services only to post, send and receive messages and material that are proper and related to the particular Communication Service. By way of example, and not as a limitation, you agree that when using a Communication Service, you will not:

- Defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others.
- Publish, post, upload, distribute or disseminate any inappropriate, profane, defamatory, infringing, obscene, indecent or unlawful topic, name, material or information. You represent and warrant that you have all the rights, power and authority necessary to grant the intellectual property rights granted herein to any content submitted.
- Upload files that contain software or other material protected by intellectual property laws (or by rights of privacy or publicity) or provide links to sites where other users can obtain unauthorised downloads, unless you own or control the rights thereto or have received all necessary consents.
- Upload files that contain viruses, corrupted files, or any other similar software or programs that may damage the operation of another's computer.
- Advertise or offer to sell or buy any goods or services for any business purpose, unless such Communication Service specifically allows such messages.

- Conduct or forward surveys, contests, pyramid schemes or chain letters.
- Download any file posted by another user of a Communication Service that you know, or reasonably should know, cannot be legally distributed in such manner.
- Falsify or delete any author attributions, legal or other proper notices or proprietary designations or labels of the origin or source of software or other material contained in a file that is uploaded.
- Restrict or inhibit any other user from using and enjoying the Communication Services.
- Violate any code of conduct or other guidelines which may be applicable for any particular Communication Service.
- Harvest or otherwise collect information about others, including e-mail addresses, without their consent.
- Violate any applicable laws or regulations.

You agree that you are responsible for your own use of the +Spaces platform, for any posts, comments, audio or text messages you make, and for any consequences thereof.

+Spaces has no obligation to monitor the Communication Services. However, +Spaces reserves the right to review materials posted to a Communication Service and to remove any materials in its sole discretion. +Spaces reserves the right to terminate your access to any or all of the Communication Services at any time without notice for any reason whatsoever.

+Spaces reserves the right at all times to disclose any information as necessary to satisfy any applicable law, regulation, legal process or governmental request, or to edit, refuse to post or to remove any information or materials, in whole or in part, in +Space's sole discretion.

Always use caution when giving out any personally identifying information about yourself or your children in any Communication Service. +Spaces does not control or endorse the content, messages or information found in any Communication Service and, therefore, +Spaces specifically disclaims any liability with regard to the Communication Services and any actions resulting from your participation in any Communication Service. Managers and hosts are not authorized +Spaces spokespersons, and their views do not necessarily reflect those of +Spaces.

Materials uploaded to a Communication Service may be subject to posted limitations on usage, reproduction and/or dissemination. You are responsible for adhering to such limitations if you download the materials.

#### MATERIALS PROVIDED TO +Spaces OR POSTED AT ANY +Spaces WEB SITE

+Spaces does not claim ownership of the materials you provide to +Spaces (including feedback and suggestions) or post, upload, input or submit to any +Spaces Web Site or its associated services (collectively "Submissions"). However, by posting, uploading, inputting, providing or submitting your Submission you are granting +Spaces, its affiliated companies and necessary sublicensees permission to use your Submission in connection with the operation of their Internet businesses including, without limitation, the rights to: copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate and reformat your Submission; and to publish your name in connection with your Submission.

No compensation will be paid with respect to the use of your Submission, as provided herein. +Spaces is under no obligation to post or use any Submission you may provide and may remove any Submission at any time in +Space's sole discretion.

By posting, uploading, inputting, providing or submitting your Submission you warrant and represent that you own or otherwise control all of the rights to your Submission as described in this section including, without limitation, all the rights necessary for you to provide, post, upload, input or submit the Submissions.

#### LIABILITY DISCLAIMER

The information, software, products, and services included in or available through the +Spaces web site may include inaccuracies or typographical errors. Changes are periodically added to the information herein. +Spaces and/or its suppliers may make improvements and/or changes in the +Spaces web site at any time. Advice received via the +Spaces web site should not be relied upon for personal, medical, legal or financial decisions and you should consult an appropriate professional for specific advice tailored to your situation.

+Spaces and/or its suppliers make no representations about the suitability, reliability, availability, timeliness, and accuracy of the information, software, products, services and related graphics contained on the +Spaces web site for any purpose. to the maximum extent permitted by applicable law, all such information, software, products, services and related graphics are provided "as is" without warranty or condition of any kind. +Spaces and/or its suppliers hereby disclaim all warranties and conditions with regard to this information, software, products, services and related graphics, including all implied warranties or conditions of merchantability, fitness for a particular purpose, title and non-infringement.

To the maximum extent permitted by applicable law, in no event shall +Spaces and/or its suppliers be liable for any direct, indirect, punitive, incidental, special, consequential

damages or any damages whatsoever including, without limitation, damages for loss of use, data or profits, arising out of or in any way connected with the use or performance of the +Spaces web site, with the delay or inability to use the +Spaces web site or related services, the provision of or failure to provide services, or for any information, software, products, services and related graphics obtained through the +Spaces web site, or otherwise arising out of the use of the +Spaces web site, whether based on contract, tort, negligence, strict liability or otherwise, even if +Spaces or any of its suppliers has been advised of the possibility of damages. because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you. if you are dissatisfied with any portion of the +Spaces web site, or with any of these terms of use, your sole and exclusive remedy is to discontinue using the +Spaces web site.

SERVICE CONTACT : [info@atc.gr](mailto:info@atc.gr)

#### TERMINATION/ACCESS RESTRICTION

+Spaces reserves the right, in its sole discretion, to terminate your access to the +Spaces Web Site and the related services or any portion thereof at any time, without notice. GENERAL To the maximum extent permitted by law, this agreement is governed by the Greek laws and you hereby consent to the exclusive jurisdiction and venue of courts in Athens, Greece. in all disputes arising out of or relating to the use of the +Spaces Web Site. Use of the +Spaces Web Site is unauthorized in any jurisdiction that does not give effect to all provisions of these terms and conditions, including without limitation this paragraph. You agree that no joint venture, partnership, employment, or agency relationship exists between you and +Spaces as a result of this agreement or use of the +Spaces Web Site. +Spaces's performance of this agreement is subject to existing laws and legal process, and nothing contained in this agreement is in derogation of +Spaces's right to comply with governmental, court and law enforcement requests or requirements relating to your use of the +Spaces Web Site or information provided to or gathered by +Spaces with respect to such use. If any part of this agreement is determined to be invalid or unenforceable pursuant to applicable law including, but not limited to, the warranty disclaimers and liability limitations set forth above, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the agreement shall continue in effect. Unless otherwise specified herein, this agreement constitutes the entire agreement between the user and +Spaces with respect to the +Spaces Web Site and it supersedes all prior or contemporaneous communications and proposals, whether electronic, oral or written, between the user and +Spaces with respect to the +Spaces Web Site. A printed version of this agreement and of any notice given in electronic form shall be admissible in judicial or administrative proceedings based upon or relating to this agreement to the same extent and subject to the same conditions as other business documents and records originally generated and maintained in printed form. It is the express wish to the parties that this agreement and all related documents be drawn up in English. The +Spaces polls, debates

and role-playing-simulations will take place until 30 June 2012. The +Spaces consortium has the right to discontinue the carrying out of the polls, debates and role-playing-simulations at any time and without prior information to the users.

#### COPYRIGHT AND TRADEMARK NOTICES:

All contents of the +Spaces Web Site are: Copyright 2010-2012 and/or its suppliers. All rights reserved.

#### TRADEMARKS

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

Any rights not expressly granted herein are reserved.

#### INDEMNIFICATION

You agree to hold harmless and indemnify the +Spaces consortium, and any of the parties involved in +Spaces, or their subsidiaries, affiliates, officers, agents, and employees from and against any third-party claim arising from or in any way related to: (a) your use of the +Spaces platform, (b) your breach or alleged breach of any of the terms, restrictions, obligations or representations under this agreement, including any liability or expense arising from all claims, losses, damages (actual and consequential), suits, judgments, litigation costs and attorneys' fees, of every kind and nature. In such a case, the +Spaces consortium or any party involved in +Spaces will provide you with written notice of such claim, suit or action.



## 10 Annex V: Report +Spaces/WeGov Workshop

### Legal challenges for FP7 projects: a +Spaces and WeGov workshop

Part of the Samos Summit 2012

Wednesday 04.07.2012

The workshop was organised by +Spaces in collaboration with the WeGov project as part of the Samos Summit 2012, and aimed at presenting issues, challenges and possible difficulties that EU research projects deal with, focusing mainly on the ones relating to legal and ethical ones. Due to some changes in the programme of the Summit, the programme chair asked us to host two additional presentations and thus two new items were added in the beginning of the workshop: a short presentation on the Open Innovation Strategy and Policy Group and a presentation on the MOSIPS project. This also limited the discussion time that was foreseen at the end of the workshop.

#### Open Innovation Strategy and Policy Group

(Anna Sadowska, EIR)

Anna presented the activities of the Open Innovation Strategy and Policy Group (OISPG) (<https://sites.google.com/site/openinnovationplatform/home>) and navigated the participants in the workshop through the initiatives of open innovation put into practice. Anna stressed the importance of the challenges among the innovation processes which incorporate external ideas, of openness of data and of the new mechanisms coming up to speed up the development of new services in Europe. During H2020 OISPG will focus its activities on validation of OI mechanisms and processes involving citizens and opening data and its effectiveness towards growth and job creation. OISPG is very interested in finding out the outcome of research projects and other initiatives which explore further the OI approach and business models based on these phenomena.

#### MOSIPS - Open data and multi-agent models for the simulation and forecast of the Public Policies impact

(Neftis Atallah, Anova IT Consulting)

Neftis presented the MOSIPS project, which is an EU FP7 project on modelling and simulation of the impact of public policies on SMEs. Neftis pointed out the difficulties that governments face in forecasting the impact of policies, which currently is considered as inadequate. She stressed the importance of MOSIPS, which aims at the creation of a tool for facilitating the decision-making process by providing the possibility to make experiments

with different socio-economic designs and the establishment of mechanisms to expose open data and boost the involvement of citizens. MOSIPS is using multi-agent systems to model the real economy based on the attributes and behaviour of each individual actors and their relations. Given the importance of SMEs in EU Economy, the tool will focused to the impact of the SME-oriented policies and they will expose the simulation results as open data. How does this expose the conflict between open data initiatives and data/privacy protection?

Sergio Gusmeroli from TXT asked what will be the test cases that will be launched in Madrid and Verona. Neftis answered that although the SMEs policies are developed at an upper administration level, different application could be implemented at the cities' level to support policy making. Besides, Verona and Madrid are cities with very different characteristics so the test cases will be different.

### **Legal and Ethical Issues relating to the use by policy makers of tools for tracking and analysing social networking discussion**

#### **(Paul Walland, IT Innovation)**

Paul Walland presented the WeGov project which aims at facilitating government policy-makers in engaging better with citizens by utilising channels citizens already use and are familiar with, such as social media like Twitter or Facebook. WeGov is developing a toolbox with web applications for search, topic analysis, discussion activity analysis and user behaviour analysis in order to identify hot topics of discussion, find key citizens, and to spot their opinions. The WeGov project was confronted with a number of legal and ethical challenges. One of the questions Paul raised was whether the problems arising were new or simply a new incarnation of an old problem? WeGov has recognised that there needs to be a balance on how we can ensure legal compliance whilst maintaining trust, since citizens must be confident that ,big brother' is not snooping on their privacy. It isn't enough to just maintain Legality, also user perception and maintenance of ethical principles will be critical. Whilst most people may agree to trading their personal data in exchange for Tesco coupons they seem to be much less willing to reveal information and personal data to the government, since they don't trust the government to protect their data. WeGov will produce a best practice Guidelines document at the end of the project in September 2012. Paul also said that the WeGov toolkit will be available via the WeGov website soon for evaluation.

### **Controllership issues in FP7 projects – example of SocloS**

#### **(Aleksandra Kuczerawy/Brendan Van Alsenoy, ICRI-KU Leuven)**

Aleksandra presented the SocloS project, which is an EU FP7 project with the objective to allow the leveraging of content from SNS (UGC and Social Graph). The use cases of the SocloS project are the use of SNS data for journalistic and media production purposes.

Aleksandra explained the concepts of controller and processor and their origin, historic background, implications of the assignment of a specific role. Aleksandra discussed the problems this complicated relation between data controller and data processor poses in the current situation of multi-level platforms, with entities involved to a different degree, on different stages, possibly from different countries. SocloS is a perfect example of complex situation with a number of entities responsible for different components, where it is difficult to apply the binary division (controller v. processor) as specified in the Data Protection Directive. Particularly in FP7 projects when these issues are often not given enough attention, should be discussed from the very beginning, possibly already in the DoW.

Questions arose from the audience with regard to the awareness of users of social media with regard to their role, as well as regarding the ownership of content when bought by a journalist.

### **Legal Issues while researching users' behaviour in virtual spaces**

#### **(Eleni Kosta, ICRI- KU Leuven)**

+SPACES is an EU FP7 project aiming at Policy making simulation in virtual spaces (virtual worlds). In +Spaces virtual spaces are classified into (a) Online Social Networking platforms (Facebook, Twitter, Blogger) and (b) 3D Online virtual worlds (Open Wonderland). The project has dealt extensively with legal issues and a final deliverable is going to be published in the end of September. +Spaces carried out an extensive review of Terms of Use and privacy notices of Virtual Spaces in order to ensure compliance of the +Spaces platform with the Terms of Use of Virtual Spaces. +Spaces also dealt with issues relating to the posting of content, the deployment of user interface, the storing and the extracting of content. With regard to the issues of data controllership (previously presented by Aleksandra), +Spaces defined clearly the roles of the project partners, and filed a notification to the Greek Data Protection Authority. Eleni finally presented the opinion of the Greek DPA on the EU FP7 research project COCKPIT, which is interesting for all European projects.

### **Privacy, Law and Social Networks - is 'consenting' a model of the past?**

#### **(Christian Hawellek, IRI-University of Hannover)**

Christian presented the CONSENT (CONsumer SENTiment regarding privacy on user generated content services in the digital economy) EU FP7 project, which aims to study the online behaviour of consumers', their attitudes toward personal privacy and the effects of contractual, commercial and technical practices on consumer's choice. CONSENT is based on the OECD definition of User Generated Content. Christian presented some results of a survey they conducted examining various aspects of consumer's behaviour in social networks, such as the correlation between age and online behaviour or to which extent users change their online behaviour depending on reading and understanding the privacy policy.

Discussions were raised on the role of minors: what is the strategy to deal with children who can't enter legally binding contracts and how can the difficulty of understanding complex legal text be overcome.

### **Discussion: The future of legal and ethical research in Europe**

The discussion part started with the question whether creating general rules for e-government engagement is necessary. The participants in the workshop found that the issues is too complex for a single rule base because of differences between different legislative systems around Europe and worldwide. Another point was raised on whether real data was necessary for R&D projects, as opposed to the need for thorough testing of publicly used systems using real data (a distinction between for example WeGov which is going to be used by policy makers in real situations compared with research projects developing the tools).

