DELIVERABLE REPORT D5.3 “Privacy Policy Framework”

collaborative project

MASELTOV
Mobile Assistance for Social Inclusion and Empowerment of Immigrants with Persuasive Learning Technologies and Social Network Services

Grant Agreement No. 288587 / ICT for Inclusion

project co-funded by the
European Commission
Information Society and Media Directorate-General
Information and Communication Technologies
Seventh Framework Programme (2007-2013)

Due date of deliverable:	30 September, 2014 (month 33)
Actual submission date:	19 October 2014
Start date of project:	Jan 1, 2012
Duration:	39 months

Work package	**WP5 – PERSONALIZATION AND RECOMMENDATION**
Task	**T5.3 – Privacy Policy Framework**
Lead contractor for this deliverable	**AIT**
Editor	**Sofoklis Efremidis**
Authors	**Sofoklis Efremidis, Iakovos Georgiou, Ioannis Christou, Jan Jones**
Quality reviewer	**Charlie Pearson (PP), Lucas Paletta (JR)**

Project co-funded by the European Commission within the Seventh Framework Programme (2007–2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

VERSION HISTORY

version	date	author	reason for modification	status
001	10.09.2014	Iakovos Georgiou	First draft version	Internal
002	16.09.2014	Sofoklis Efremidis	First consolidated version with input from OU	Internal
003	6.09.2014	Sofoklis Efremidis	Draft version for internal review	Internal
004	13.10.2014	Sofoklis Efremidis	Final version after internal review from PP and JR	Internal

MASELTOV partner			organisation name	country code
01	JR		JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH	AT
02	CUR		CURE CENTRUM FUR DIE UNTERSUCHUNG UND REALISIERUNG ENDBENUTZER-ORIENTIERTER INTERAKTIVER SYSTEME	AT
03	AIT		RESEARCH AND EDUCATION LABORATORY IN INFORMATION TECHNOLOGIES	EL
04	UOC		FUNDACIO PER A LA UNIVERSITAT OBERTA DE CATALUNYA	ES
05	OU		THE OPEN UNIVERSITY	UK
06	COV		COVENTRY UNIVERSITY	UK
07	CTU		CESKE VYSOKE UCENI TECHNICKE V PRAZE	CZ
08	FHJ		FH JOANNEUM GESELLSCHAFT M.B.H.	AT
09	TI		TELECOM ITALIA S.p.A	IT
10	FLU		FLUIDTIME DATA SERVICES GMBH	AT
11	BUS		BUSUU ONLINE S.L	ES
12	BUS_UK		BUSUU ONLINE Ltd.	UK
13	FUN		FUNDACION DESARROLLO SOSTENIDO	ES
14	DAN		VEREIN DANAIDA	AT
15	MRC		THE MIGRANTS' RESOURCE CENTRE	UK
16	PP		PEARSON PUBLISHING	UK
17	ATE		AUSTRIAN INSTITUTE OF TECHNOLOGY	AT

CONTENT

1. EXECUTIVE SUMMARY

This document reports on the privacy issues of the MASELTOV platform. In the context of MASELTOV privacy becomes a primary issue exactly because of the particularities of the user target group, i.e. new coming immigrants who are in the process of adapting to their new host environment and may possibly refrain from being socially visible. As a result MASELTOV gives high priority to the privacy of the potential users of the platform and provides the mechanisms for allowing them a good level of control over it. This document reports on the technicalities and the approach taken towards security and privacy protection of MASELTOV users. It presents the designs and algorithms used for that purpose and for the secure handling of personal data, their storage and transfer between components of the User Profile. It also gives an overview of the privacy policy framework in effect at the European level.

2. OVERVIEW

Privacy issues are handled in the User Profile, which is responsible for manipulating personal data, user preferences, as well as all user contextual information that is carried through a number of events generated by the various MApp applications.

This document is a report on the privacy issues that are supported by the User Profile of the overall MASELTOV platform. It provides details on its architecture, functionalities and algorithms used in order to protect users' personal data and provide a level of privacy for them. The User Profile is the core component in MASELTOV platform that handles user's personal data, provides user's information to other MApp components, handles transmission of user's data from and to the back-end servers, and finally stores the user's data in the back-end server database.

The overall architecture of the User Profile and the Recommender system are reported in Deliverable D5.2 "User Profiling and Personalization" and is shown in Figure 1. The figure shows that the User Profile is the central component of the overall architecture and the single point of interfacing with the rest of the MASELTOV applications and services. Moreover it shows that both the User Profile and the recommender comprise a client and a server component. The client User Profile component forwards the events and notifications it receives from other MApp applications to the back-end User Profile, which eventually logs them in the back-end database for further processing. For example, the recommender queries the database for events that trigger recommendations to be presented to the user.

A number of privacy and security issues arise, which the User Profile has to take into account so as to safeguard the authenticated access to user accounts, controlled collection of user contextual information, safe handling of the user personal data, and the secure transmission of user-related data back and forth between the client and the server components.

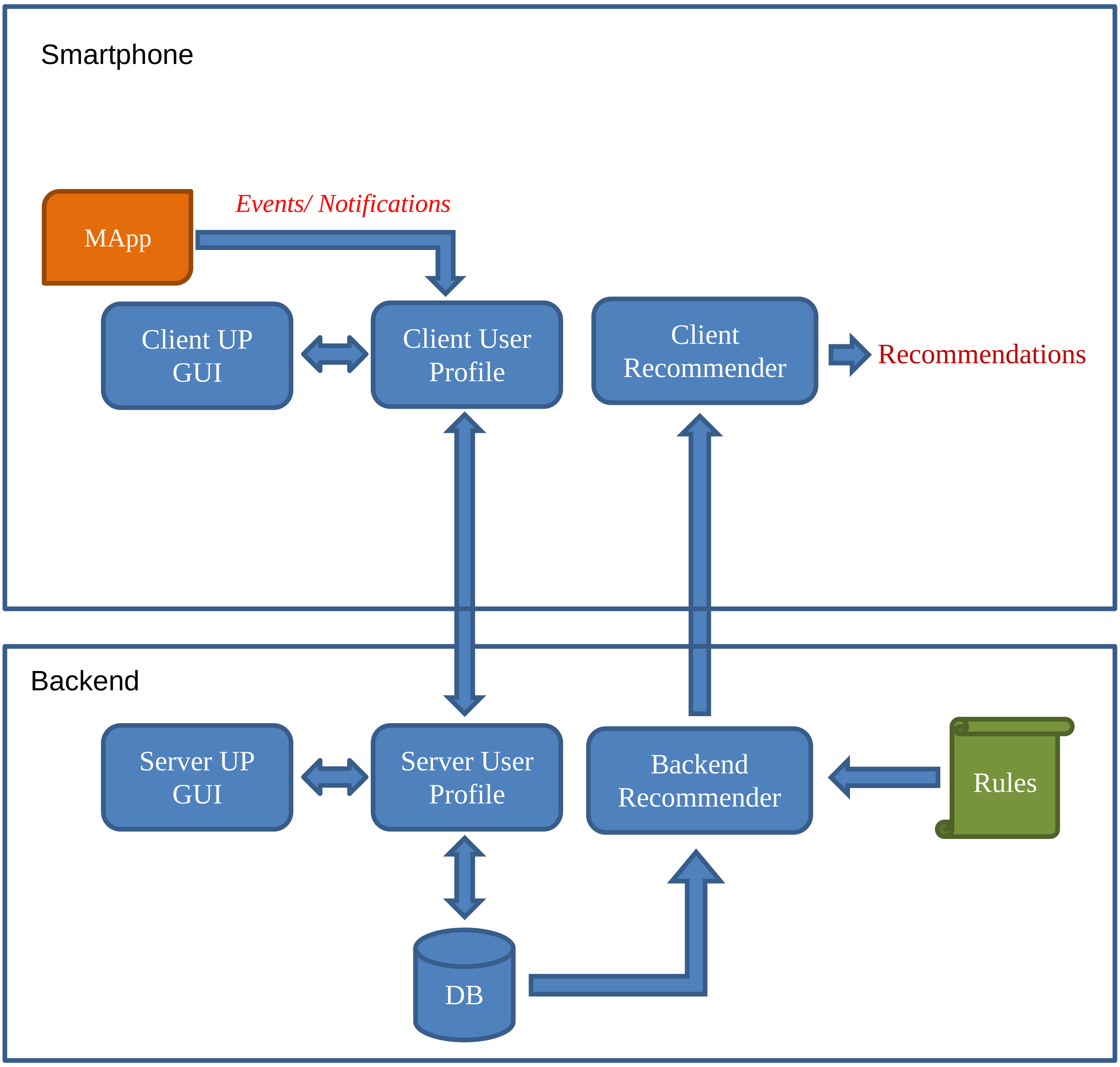


Figure 1: Reference Architecture of the User Profile and the Recommender System.

The User Profile provides support for user privacy through a number of functionalities:

- User registration: users may register for use of the platform without providing any personal information, like name or any ID number. Only a valid email address is required, which does not reveal the actual user identity. The result of the registration is the creation of a password-protected account that may be used to access the various MASELTOV functionalities.
- Targeted messages during registration: the user registration process forces users to read the privacy policy statement of the platform. As a result users are informed at the time of registration about the platform's privacy policies.
- Validation of email address: The User Profile protects users from impersonation. The email address registered by a user during the registration process is validated by the User Profile. A validation code is sent to that email address that must be further used by the user in order to validate the address and activate the account.

- User authentication: users may log into the platform using their email address and a password. To allow access to the platform to users who do not want to register (and as a consequence provide a valid email address), anonymous registration is supported by the User Profile.
- Security protections against attacks: the User Profile allows a password to be used for a fixed number of logins. After this number of logins is exceeded, a new password must be selected.
- Protection of the user password: the password the user selects is never transmitted in the clear between the client and the server. Instead a hashcode of the password is communicated. To even protect the communicated hashcode, a new one is used for each login.
- Protection of the communicated user data: user data (events and preferences) that are communicated over the network are secured. The corresponding user identity is never sent in clear, therefore, the communicated data cannot be associated to a user. Optionally the data may be transmitted in encoded form, so as to ensure no statistical processing by eavesdroppers is possible.
- User control over collection of contextual information: a number of configuration switches are available to the users that allow them control over the level of contextual information that may be collected by the platform for the purpose of generating personalized recommendations. This mechanism allows users to progressively allow wider amounts of contextual information to be collected (and therefore more targeted recommendations to be generated) as trust is gained for the platform.
- Transparency of use of personal data: the User Profile provides additional information to users for the purpose of each of the user data and preference fields and their intended use. Therefore, users are fully informed before providing this information to the User Profile.

The following chapters give an overview of the privacy issues, trust, and data security, an overview of the privacy framework at the European level, and the technicalities that have been implemented in the MASELTOV platform for the support of the privacy issues as presented above.

3. TOWARDS A PRIVACY POLICY FRAMEWORK

3.1 THE IMPORTANCE OF PRIVACY, TRUST AND DATA SECURITY

The tools and services being developed for the MASELTOV application (MApp) present a number of privacy, trust and data security issues. At a focus group in 2012 privacy, trust and data security were raised as a main concern by potential users, and as having the potential to prohibit use. It is therefore, essential that these issues are addressed by each tool or service provider and integrated into the MApp system architecture.

The issues identified include the following:

- The development of apps in different EU countries that have different political systems and different legal restrictions. Furthermore, different tools and services will be used by users in different countries, and if this data is shared it is likely to cross national boundaries to link with the service provider. In current legislation (discussed below) each EU country can interpret EU guidance on data protection in their own way. Consequently data input in one country may be subject to the legal regulations of the service providers governed by a different set of regulations.
- To achieve the aim of social inclusion, users need to be assured that their data is secure.
- The need to assure users of the privacy of any data they input into a tool or service.
- The need for users to understand the risks involved in sharing personal data through the MApp.
- The need to ensure users are aware of how any data they provide will be used, i.e. to make personal recommendations, or if BIG data is to be obtained, provide an explanation of how and why the data is to be used on a broader scale.
- Users need to be informed about circumstances when MASELTOV might be required to breach confidentiality, i.e. where a legal intercept is necessary, for example, in the UK.
- Any written guidance or information needs to be written in simple language so that users can easily understand the issues.
- For users whose language skills are limited, it will be necessary for any information or guidance on privacy, trust and data to be available in the user’s mother tongue and access to a translator or translation tool made available.
- Many MApp users may be considered to be in a vulnerable position. Informed consent should be obtained, but this could prove difficult as users may not be aware of data privacy and security issues, especially if recently arrived in the host country from outside the EU. They may require additional support or guidance before they are able to give informed consent. A point of contact should be available to deal with any issues relating to privacy, trust and data security concerning the MApp. Details of the point of contact should be easy to find within the MApp.
- Informed consent will help to reassure users about what will happen to any data they provide. Informed consent should link to a description of the purpose of the MApp.
- The need for users to understand when and where it is appropriate to take photographs or videos.

- It is known that some migrants do not have a phone of their own and use other people's phones. In such situations, it is not clear what steps can be taken to ensure privacy, trust and data security of the owner. The complexity of the security risks increase. For example, mobile devices can reveal aspects of a person's identity such as their GPS location and the device model, without the owners' knowledge or consent. (Traxler and Bridges, 2004, cited in Lally, V., Sharples, M., Tracey, F., Bertram, N. and Masters, S. (2012).
- The provision of examples of good practice.

3.2 DATA PROTECTION DEFINITIONS

This section contains some useful definitions related to Data Protection that appear in Directive 95/46/EC [7].

- **Personal data** is 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.
- **Processing of personal data** (processing) is any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **Informed consent** is said to have been given where there is a clear appreciation and understanding of the facts, implications, and consequences of an action.

3.3 BACKGROUND OF EU DATA PROTECTION AND RELEVANCE TO THE MAPP

Research has shown that 92% of Europeans say they are concerned about mobile apps collecting data without their consent and 70% are concerned about the potential use that companies may make of the information they disclose [10].

EU member states are currently guided by the Data Protection Directive 95/46/EC [7], and its subsequent amendment in 2003 [8], for the protection of personal data. Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data.

In view of the technological revolution that has taken place in the 21st Century, many of the rules in the EU Directive (and member state legislative documents) are now out of date and new rules are necessary. Therefore, on 25 January 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online data protection rights and boost Europe's digital economy. In terms of MASELTOV, a Directive written in 1995 (and updated in 2003) will not cover all the intended data usages intended for its range of tools and services. One of the main issues regarding Directive 95/46/EC is that it is a Directive, rather than a Regulation; a Directive that allows member states to interpret the guidelines in their own way. Hence, one of the main changes agreed by the European

Parliament is that the new regulation becomes law in all EC countries, rather than a directive, to remove the fragmentation that has resulted from different interpretations of the EU 1995 Data Protection Directive, and enable any EU consumer who has a complaint against a company in an EU country that is not their own, to act with ease. The EU Data Protection Newsroom provides up to date information on developments concerning the EU Data Protection reform and a series of factsheets. The factsheets entitled ‘How will the EU’s reform adapt data protection rules to new technological developments?’ and ‘How will the data protection reform affect social networks’ are particularly pertinent to MASELTOV.

At a meeting in Brussels on 24/25.10.13 European heads of state and government committed to a ‘timely’ adoption of the new data protection legislation and the EC made a commitment to complete the ‘Digital Single Market’ by 2015. For further information please see Section 1.6 in the Conclusions of the European Council meeting.

More recent progress on the reform can be viewed in a factsheet on a Plenary vote taken in March 2014. It is noted that the European Parliament now views EU citizens as being at the heart of the data protection reform.

3.3.1 PRINCIPLES OF THE PROPOSED DATA PROTECTIONS REFORM

The factsheet on the Plenary Vote also outlines four new rules to enable EU citizens to retain control of their personal data. These are as follows:

- **Data protection first, not an afterthought:** ‘Privacy by design’ and ‘privacy by default’ will become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks.
- **Putting you in control:** When consent is required to process personal data, people must be asked to give it explicitly. Businesses and organisations will also need to inform you without undue delay about data breaches that could adversely affect them.
- **A right to be forgotten:** When you no longer want your personal data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. This is about empowering individuals, not about erasing past events or restricting freedom of the press.
- **Easier access to your own data**: A right to data portability will make it easier for you to transfer your personal data between service providers.

It is worth noting that on 8.4.14, the European Court of Justice (ECJ) rejected a Data Retention Directive that was introduced in 2006 to help fight terrorism and crime. The ECJ said “it interfered with the functional right to privacy and protection of personal data”. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf. In the UK, which objected to the Data Retention Directive, a new Data Retention and Investigation Powers Bill (DRIP) was passed and came into force on 18.7.14. Any data obtained via MASELTOV therefore, needs to be retained according to the relevant law.

MASELTOV intends to track users’ interactions with the tools and services that motivate and support informal learning in several EU countries including the UK, Austria, Spain and Italy, to improve social inclusion of new EU immigrants. This means that data obtained from people using a service in one country may well be stored with a service provider in a different country. So, for example, Recommendation services (WP5) will be provided by AIT in Greece, Community Building Services (WP8) will be provided in Italy and the UK; so a new Data Protection reform that covers all EU member states will be beneficial for MASELTOV and ensure the MASELTOV Privacy Policy Framework and guidance provided for its users is straightforward.

There are indications that the new reform should become law in 2015, although in view of its complexity, this may take a little longer. Therefore, if any of the MASELTOV tools and services are to become products, or have any impact beyond the project, it is recommended that they comply with this proposed legislation.

3.4 SUGGESTED POINTS FOR A MASELTOV PRIVACY POLICY FRAMEWORK

The following list contains a set of suggestions for the MASELTOV services following the relevant EU regulations.

- Users are provided with comprehensive and easy to understand information about security settings.
- Recommender service – Inform and warn users of the consequences of providing personal information (pros and cons), explaining how to turn off the service when needed and to provide tips to avoid risky situations (See D1.2).
- Geo-radar – Inform and warn users on the consequences (pros and cons) of being tracked, explaining how to turn off the service when needed and giving tips to avoid risky situations (See D1.2).
- All MASELTOV tools and services promote ‘privacy by design’ and ‘privacy by default’. Data protection safeguards are built into all products and services.
- Privacy information is given to users in two ways:
  i) In a yes/no icon-based table, and presented in easy to read text in own language
  ii) In a detailed note. Any information provided needs to be accessible to users.

Volunteers are to be trained to understand, and if necessary interpret, the more detailed note.

- Users are asked for their informed consent on the purposes for which personal data may be used after they have read the privacy information in at least one of the above two ways. To obtain their consent, they are required to agree to the Terms and Conditions as outlined in the disclaimer text before using the MApp tools and services. If they are able to use the tools and services without providing personal data, a clear explanation of which tools they can use in this way needs to be provided and a selection field for this option also provided.
- If users decide they no longer want the MApp to process their personal data, and there are no legitimate grounds for retaining it, the data will be deleted.
- Users have a right to access any personal data held by any of the MASELTOV tools and services.
- Users are provided with a strategy for reporting abusive or unacceptable forum posts.
- Users are informed about legal restrictions concerning use of media such as photography and video-making in their country and in the country of the service provider.

3.5 PRIVACY ISSUES CONCERNING SPECIFIC MASELTOV TOOLS AND SERVICES

3.5.1 USER PROFILE (MY PROFILE)

- Users are informed about which information is essential for engagement in a tool or service.
- Users are informed about the benefits of providing additional information through preferences and personal data.
- Users should be reminded about the risks involved in sharing personal data.

3.5.2 FORUM

- Provide a netiquette or Code of Conduct to inform users about how to interact in this social network.
- Provide a trained/experienced forum moderator.
- Ensure users are provided with a strategy for reporting abusive or unacceptable forum posts.
- Keep a record of issues that transgress the Code of Conduct.

3.5.3 INFO

- No information available.

3.5.4 HELP RADAR, PEDESTRIAN NAVIGATION, NAVIGATION AND PLACES OF INTEREST

- Users need to be aware that these services require their GPS location to function effectively.
- Inform users about the consequences (pros and cons) of being tracked.
- Provide an easy to read explanation on how to switch GPS locations on and off, when not required.
- Warn users about potential risks associated with GPS tracking.
- Provide tips for avoiding risky situations.

3.5.5 TRANSLATION TOOL (TEXT LENS)

Users should be informed about legal restrictions concerning photography. [14] provides information on worldwide privacy laws in relation to street photography. It gives a country-by-country guide and further relevant links.

In the UK Legal Restrictions on the right of individuals to take photographs include photographing buildings in the following circumstances:

- Individuals cannot take pictures of buildings used for commercial or private purposes that are on privately owned land unless you have permission, e.g. privately owned shopping malls or complexes. (Copyright Law).
- Individuals can’t take pictures of places whether inside or outside that might present a security threat e.g. inside police stations, military establishments, royal or presidential palaces, at an airport, etc.
- Individuals cannot take pictures of building where permission is required, e.g. museums and art galleries, doctor’s surgeries or in a court of law.
- Individuals who are taking pictures in the above places, need to be aware that they may be asked what they are doing and why.

3.5.6 LANGUAGE LEARNING

Language learning in social networks

- Provide guidelines on communication with other people in the forum. Further details appear in "the Forum" draft Ethical Code of Practice _UOC draft 1 (internal document)

3.5.7 RECOMMENDATIONS

- Inform users about the benefits and risks of providing personal information.
- Explain how to switch off the service if necessary.

A record should be kept of events that transgress the Code of Conduct or Privacy Policy. It is recommended that data privacy, trust and security is monitored and evaluated on a regular basis, and remedial action taken where possible. This may include amendments to the Code of Conduct or Privacy Policy and/or software updates to improve security if necessary. Whilst the project has endeavoured to consider all potential threats to data privacy, trust and security with technology changing so fast, it is not possible to foresee all future risks. The ethics associated with these themes must be negotiated as new technologies are developed.

The target group of users for MASELTOV, recent immigrants to the EU from outside, also poses one issue that is yet to be addressed, i.e. how MASELTOV can protect the privacy, trust and security of individuals who use its tools and services and who may not yet have EU citizen status. There may also be the potential for illegal immigrants to use the tools and services.

MASELTOV's Privacy Policy Framework needs to reflect the relevant issues and solutions raised in D1.6 Strategy for Ethical Issues (WP1). See draft Ethical Code of Practice. The proposed Privacy Information Disclaimer will need to address all of the information covered in D5.3: Privacy Policy Framework. Currently it reads as:

> Some MASELTOV services need to process collected data to work properly. For this reason, each service will inform you why it needs what kind of data from you. For basic functionality MASELTOV only needs a user name and the city you live in. To benefit from all services and to receive recommendations, we need to know the location of your device and some more information that you can enter under My Profile.
>
> We will not share your data with anyone for any reason. Your data will be stored anonymously and only used within the MASELTOV project.
>
> Please note that MASELTOV is a research prototype and not a fully advanced product. Thus, we cannot guarantee accurate functionality the whole time. (15.8.14)

3.6 PRIVACY REQUIREMENTS FOR MOBILE APPLICATIONS

[16] addresses end-users' privacy requirements on mobile applications (apps). The authors emphasize that traditional privacy requirements elicitation methods cannot be used to represent and analyze mobile users' privacy requirements as mobility adds another level of contextual variation to the socio-cultural factors that form the foundations of privacy on non-mobile computing devices. The authors suggest that system designers and organizations can easily become isolated from end-users' perception of privacy when mobile app users' context changes frequently and unpredictably, and they warn that omitting these privacy requirements may have an impact on how well a system is adopted or utilized. They argue that privacy

requirements are emergent requirements that need to be elicited and analysed from qualitative reports of the user’s experience of the application, which allows data capture through the use of Use Cases that can also illustrate privacy violations. They have developed and evaluated a Privacy Requirements Distillation approach through empirical studies with end users. The main aim of the distillation is to both equip and assist software engineers with analytical tools and techniques and also, to provide process guidance on the extraction of privacy requirements from qualitative data which can be used in the design of privacy-aware software systems.

Their Case Study: Mobile Facebook, which illustrates the application of the distillation approach, demonstrates how the process can help software engineers derive privacy requirements that address end-users’ privacy concerns. Such concerns could be used to improve the design of privacy functionality in a software system.

4. USER PROFILE PRIVACY POLICY

This chapter presents the approach taken by the User Profile towards implementing the privacy policies for the protection of user data and the mechanisms employed for that matter. The MASELTOV platform takes a careful approach towards the fact that migrants must feel secure and confident when providing their personal information that is requested for the proper functioning of the platform. In order for the user to use all of the provided services (a) they must know why the MASELTOV platform requires to know each one of their personal information, (b) they must be sure how this information is stored and transmitted securely between the device and the backend servers, and (c) they must understand how specific functionalities can provide them with added value services and so they consent so that Mapp can report their location, their social interaction etc. back to the recommender.

The User Profile is the main repository and the component responsible for storing and transmitting the user's data. The User Profile provides a secure scheme to (a) register users, (b) handle login and logout operations whenever the user wants to, (c) receive data produced from the other Mapp components, transmit them to the back-end server and store them into the back-end database. The following chapters give details of the mechanisms that are employed for the secure handling of user data and their transmission between the Android client and the back-end server.

4.1 NO USER IDENTITY

All operations between MApp components are performed using the currently logged in user provided by the virtual session that is created when the user is successfully logged in. This happens after a secure authentication that uses rolling password hashes and hashed username (the user's email is not transmitted in plain text). The User Profile takes all precautions to refrain from exposing the user's email address and also to ensure that the transmitted password is not exposed to external attacks, which may result in impersonation of the user.

The real identity of a user is not known even to the MASELTOV platform. A user is never asked to provide their name, surname, or any official ID number (passport, driver's license, tax id, etc.). A user registers on the platform with their email address, which bears no association to the actual user identity. Of course if a user chooses john.smith@gmail.com as their email address, and registers with it at the MASELTOV platform it follows that they have no issue about revealing their actual name. On the other hand one can choose a3dfclt5@gmail.com, which reveals no information about their actual name. In addition to the user name, a user is asked for a nickname during registration, which he/she can use to be announced to other users, for example when he/she participates to the forum. The nickname can be anything the user chooses and it also has no correlation to the user's identity. More than that the user's email and nickname have no apparent correlation with one another, therefore, users never see or get hold of the email of another user.

In addition to the email, password, and nickname, the only mandatory information that a user is asked is the city of residence for enabling MApp services like the POIs. All other fields of the user preferences are optional. User's preferences that are declared through the User Profile are mainly used to improve the quality of recommendations. They are made available to other MApp components through the User Profile Content Provider.

If all the above are still not enough to convince a user about the approach taken by the User Profile regarding user identity, anonymous registration is also supported, which allows users to use the platform's functionalities without even the need to provide their email address, giving them the option of total anonymity. In this case the User Profile creates a fake account to allow users to use the functionalities of the platform. The drawback with anonymous registration is that a user has to use the same device for each login, whereas with normal registration a user can login from different devices.

In summary, the User Profile is careful enough to maintain no information about the user identity, or even allow the discovery of the user's identity from other user data provided.

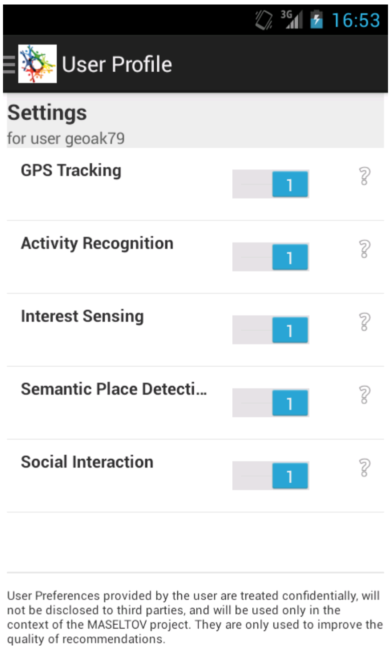
4.2 EMAIL VERIFICATION

As was noted in the previous section, the User Profile requests and maintains the email address as the user's only identity. To defend against impersonation attacks the User Profile verifies the address. To complete the registration process the User Profile sends a message to the user's email address with a link that must be used to activate the user account. Upon successful activation the user can use the services of the MASELTOV platform, while his/her real identity remains unknown.

4.3 USER CONTROL OF CONTEXTUAL INFORMATION

The User Profile places the user at control of the contextual information that he/she allows to be collected about him/her. Contextual information is generated by a number of sources on the Android device. For example the user's location is picked and reported by a background service that runs periodically and queries the device's GPS receiver. User actions like the use of TextLens and translation, search in the info component, participation in the forum, etc. form part of the user's context and result into the generation of information that is sent to the User Profile for further storage and processing.

The User Profile gives the user the option to selectively allow or disallow the collection of contextual information through a number of switches that are accessible from User Profile Settings tab. The User Profile Settings allow users to approve or deny the collection of contextual personal information like the user's geolocation, his/her social interaction with other users in the MASELTOV platform etc. Figure 2 shows the five switches that can be set to on or off by the user for controlling the contextual information he/she allows to be collected by the Android client.



16:53

User Profile

Settings
for user geoak79

GPS Tracking 1 ?

Activity Recognition 1 ?

Interest Sensing 1 ?

Semantic Place Detecti… 1 ?

Social Interaction 1 ?

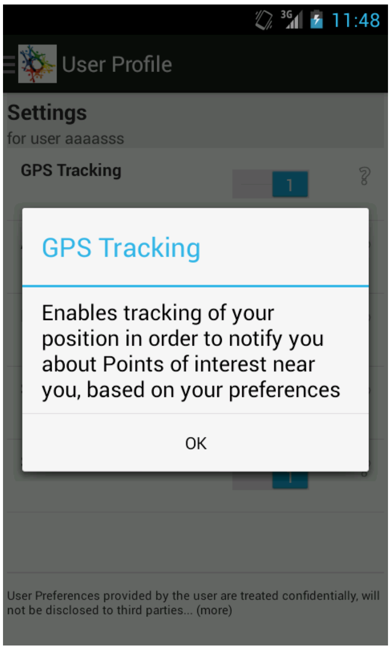
User Preferences provided by the user are treated confidentially, will not be disclosed to third parties, and will be used only in the context of the MASELTOV project. They are only used to improve the quality of recommendations.

Figure 2: User Profile switches for controlling the collection of contextual information.

The interpretation of the five switches are as follows:

- GPS tracking: Enables tracking of your position in order to notify the users about Points of Interest near you, based on your preferences. The location service performs a check every five minutes. If the current position (geolocation) is five hundred meters away from the last saved position then the service creates a new event to the User Profile Content Provider in order to be processed by the back-end Recommender and to suggest a Point of Interest to the user. By switching this setting off, the position tracking will be disabled and no events will be transmitted to the recommender. By switching this setting back on, there is no way to retrieve the user’s path while the setting was off.
- Activity recognition: Detects the optimal timing for recommendations by sensing the current type of movement, i.e. when a user walks, or is in a bus or enters a building.
- Interest Sensing: Helps to deliver personalized recommendations by collecting interests from the browser search history, browser bookmarks and frequently visited places.
- Semantic Places Detection: Enables daily reflection on places visited as well as recommendations for places.
- Social Interaction: Helps to get into contact with other people by detecting the amount of communications on the phone (text messages, calls).

As shown in the figure above, for each of the switches the form provides an explanatory text that pops up after tapping on the question mark symbol. Figure 3 depicts the explanatory text for the GPS tracking switch.



Enables tracking of your position in order to notify you about Points of interest near you, based on your preferences

User Preferences provided by the user are treated confidentially, will not be disclosed to third parties... (more)

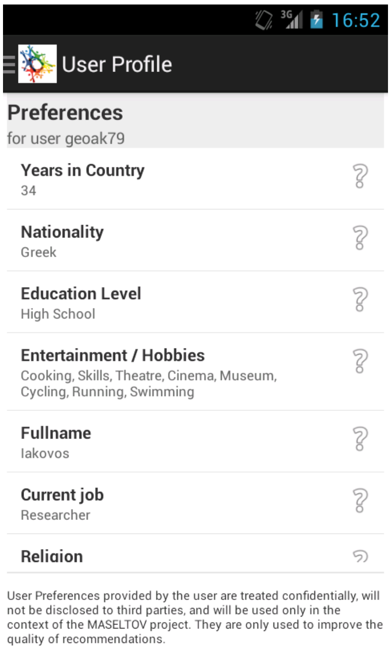
Figure 3: Explanatory text for the GPS tracking switch.

4.4 SECURE COMMUNICATIONS OF THE USER CONTEXT

Events transmitted to the server are sent using an API that expects a hashed string of the user’s email that is used to authenticate him/her along with a password hash that the sending application uses. The hashed password is the same as the one used during user login. The result is that no association between the transmitted contextual data and the user for whom they have been produced can be established. Details of the mechanisms that are employed by the User Profile for the secure handling of user’s contextual information are presented in subsequent chapters.

4.5 USER PROFILE EXPLANATORY TEXTS

The User Profile maintains a structure that contains the user preferences; optional information the user may provide that facilitates the generation of personalized and targeted recommendations. Figure 4 depicts the Preferences tab, which shows, along with each preference, a question mark that, when tapped, brings a pop up window that contains an explanatory text for the purpose and use of the respective preference, similar to that shown in Figure 3. This approach has been designed so as to provide the user all information that he/she may need for deciding if he/she wants to supply data for the corresponding preference field. It should be understood that the more information regarding user preferences is available to the recommender, the more specialized the recommendations it produces will be.



Preferences
for user geoak79

Years in Country
34

Nationality
Greek

Education Level
High School

Entertainment / Hobbies
Cooking, Skills, Theatre, Cinema, Museum, Cycling, Running, Swimming

Fullname
Iakovos

Current job
Researcher

Religion

User Preferences provided by the user are treated confidentially, will not be disclosed to third parties, and will be used only in the context of the MASELTOV project. They are only used to improve the quality of recommendations.

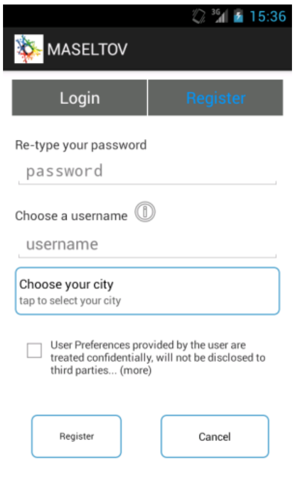
Figure 4: User Preferences Tab.

4.6 USER PROFILE STATEMENTS ON PRIVACY

As noted in a previous section the User Profile puts the user in control of how private information will be handled. The user is notified for the privacy policy that is implemented by the User Profile in several instances:

(a) During registration. The user must accept the terms by clicking on a mandatory checkbox of the form (as shown in Figure 5 and Figure 6) in order to proceed.

(b) In the User Profile. At the bottom of the screen (Figure 7) the user can tap and read the whole text on a scrollable dialog box (Figure 8).



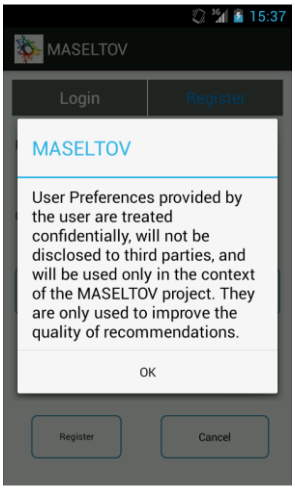
Re-type your password
password

Choose a username
username

Choose your city
tap to select your city

□ User Preferences provided by the user are treated confidentially, will not be disclosed to third parties... (more)

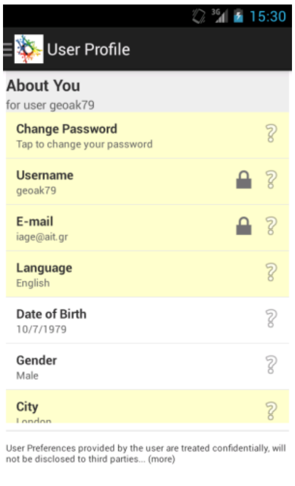
Figure 5: Privacy checkbox in registration screen.



MASELTOV

User Preferences provided by the user are treated confidentially, will not be disclosed to third parties, and will be used only in the context of the MASELTOV project. They are only used to improve the quality of recommendations.

Figure 6: Privacy dialog box in registration screen.



User Profile

About You
for user geoak79

Change Password
Tap to change your password

Username
geoak79

E-mail
iage@ait.gr

Language
English

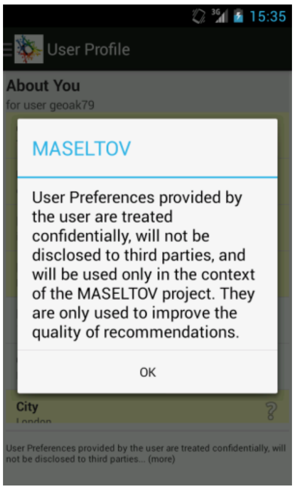
Date of Birth
10/7/1979

Gender
Male

City
London

User Preferences provided by the user are treated confidentially, will not be disclosed to third parties... (more)

Figure 7: Privacy text at the bottom of the User Profile.



MASELTOV

User Preferences provided by the user are treated confidentially, will not be disclosed to third parties, and will be used only in the context of the MASELTOV project. They are only used to improve the quality of recommendations.

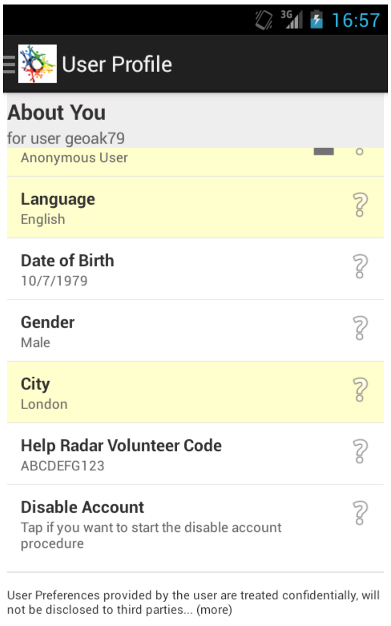
15:35
User Profile
About You
for user geoak79
OK
City
London
User Preferences provided by the user are treated confidentially, will not be disclosed to third parties... (more)

Figure 8: Privacy dialog box in User Profile.

4.7 ACCOUNT DELETION

The User Profile gives the user the option to delete their account at will. In this case all data for this user is removed from the back-end server and no record of them is kept any longer. Account deletion implements the users' right to be forgotten in case they do not want to use the MASELTOV services any longer.

Figure 9 shows the option for disabling the account in the "About you" form. When selecting the option a new form like the one shown in Figure 10 is popped up to confirm the user action.



User Profile

About You
for user geoak79

Anonymous User

Language
English

Date of Birth
10/7/1979

Gender
Male

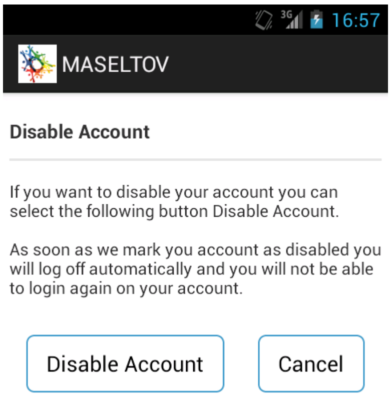
City
London

Help Radar Volunteer Code
ABCDEFG123

Disable Account
Tap if you want to start the disable account procedure

User Preferences provided by the user are treated confidentially, will not be disclosed to third parties... (more)

Figure 9: Account Disabling Option.



MASELTOV

Disable Account

If you want to disable your account you can select the following button Disable Account.

As soon as we mark you account as disabled you will log off automatically and you will not be able to login again on your account.

Figure 10: Account Disabling Confirmation.

5. USER DATA SECURITY ON THE DEVICE

5.1 REGISTRATION PROCEDURE

Users who wish to use the MASELTOV platform have to register first. MASELTOV provides two ways for one to register and get access:

(a) Normal registration: users must provide their email address, a required password, a required nickname and their city.

(b) Anonymous registration: users may register anonymously, by entering only a required nickname and their city.

For registering users, the User Profile client communicates with the back-end server via the MASELTOV User Profile API and attempts to create the user account. If the account is created successfully then the user is notified and they can subsequently log into their account. If on the other hand the user attempts to create another account using the email address or the nickname of an existing one the server returns an error message. Security issues of the back-end API communication are discussed in the following sections.

5.1.1 NORMAL REGISTRATION

Users who have registered by providing their email address and choosing their own password may login to the MASELTOV platform from any Android device that has the Mapp installed. By registering with MASELTOV, users can select their own password which must be between 5 and 15 characters long and may contain alphanumeric characters i.e. Latin characters (lower case or upper case) and numbers. In order to prevent a mistyped password, the application requires from the users to enter their password twice.

The users must also select a nickname that will be used in all MApp components to identify them, while at the same time maintain their anonymity. The Forum and the Help Radar make use of the nickname to refer to users. So users can login using their email address and communicate with other users using their nickname.

5.1.2 ANONYMOUS REGISTRATION

For anonymous registrations the client application creates a fake email and password based on the Android's ANDROID_ID constant. ANDROID_ID is a constant provided by the Android's Settings.Secure Class [1], which holds system settings and system preferences that applications can only read but not alter. These preferences can only be modified explicitly through the system UI or specialized APIs but cannot be modified directly by applications.

ANDROID_ID is a 64-bit number (as a hex string) that is randomly generated during user's first set up of the device. This id cannot be changed for the lifetime of the user's device but can be changed during a factory reset on the device. Android 4.2 and higher allow for multiple users on a single device, and in this case each user has a different device ID and so a different unique ANDROID_ID [2].

The fake email address is created as ANDROID_ID@demo.maseltov.eu. The password is created by hashing the fake emails using MD5. By using anonymous registration the user cannot be traced even at the email level since the platform does not know the user’s email address and the platform cannot identify the user’s ID by the ANDROID_ID.

The major limitation when registering anonymously is that the user can only access his/her account from the specific device from which it was registered, i.e. the user cannot access the account from another device or even from a new device that he/she may purchase in the future. Nevertheless, a user can still register anonymously from another device, thereby creating a fresh anonymous account.

5.2 LOGIN PROCEDURE

In order to use the applications of the MASELTOV platform the user must hold an active account and be authenticated via the Login screen. All MApp components perform a check with the User Profile Content Provider (UPCP) to ensure that the user is logged in and the virtual session is active. In case UPCP reports that this session does not exists any more the MApp components redirect the user to the Login screen.

The login screen on MASELTOV requires the user’s email address and the current password. As soon as the user is authenticated the application maintains the virtual session and keeps him/her logged in until the user decides to log out. Anonymous users need only press the Anonymous Login button, and the User Profile will attempt to login using a fake email and password as described above.

5.2.1 DATA SAVED DURING LOGIN

As soon as the user gets authenticated the User Profile and Recommendations components collect a number of data related to the structure of the available preferences, the data for the currently logged in user, the events sent by other MApp components as well as recommendations produced for the user.

5.2.1.1 STRUCTURE OF THE AVAILABLE PREFERENCES

The User Profile retrieves the structure of the user’s data from the backend server while the login form appears on user’s screen. This approach provides flexible manipulation of the user preferences as it allows dynamic structures that can be defined and updated from the backend administration GUI. The structure of the user preferences fields (example shown in Appendix A) is communicated as a JSON object. The URI for this action is

http://maseltov.ait.gr/maseltov/wservice/upfields/<LANGUAGE>/long

where <LANGUAGE> is the two letter representation of the language (following the ISO 639-1 standard). The language must be one of the MASELTOV available languages as described in API action for the available languages available in the following URI

http://maseltov.ait.gr/maseltov/wservice/langs

The user preferences data structure JSON object describes all information about the available user preferences fields including the field ID, the field type, field’s description (in queried language) and available options in case the fields contains multiple options.

In is noted that the JSON object contains no specific user-related data, only a map of the available fields, the name an type of each field, their nesting structure, and so on. As soon as the user successfully logs into the MApp, these fields will be populated with the currently logged-in user's selected values and will be stored in the Android client as described in the following section.

5.2.1.2 USER DATA

These data are stored in eight variables using the Android's SharedPreferences Interface [4]. SharedPreferences is an Interface for accessing and modifying preference data saved in Android's data folder for the specific application. These values are stored using the MODE_PRIVATE [5] constant so that only the MASELTOV client application can access these values. According to Android Developer Website, MODE_PRIVATE is the mode, where the created file can only be accessed by the calling application. This ensures that all saved information will be available only to MASELTOV and no other application can steal the user's data. This information can be manually removed from the device by clearing data from the Application Settings→MASELTOV from the Android's menu. Table 1 shows the data stored for each user upon login.

Table 1: List of variables that hold user-related data stored locally during logged in session.

Variable	Description
MASELTOV_USER_ID	Holds an Integer and this is the currently logged in user's ID
MASELTOV_USER_NAME	Holds a String and this is the currently logged in user's email
MASELTOV_USER_N	Holds an Integer and is the last n number received during last login (n is used as the challenge during password calculation in Lamport's authentication scheme)
MASELTOV_USER_PASSWORD	Holds a string that is the hashed password created during last login communication. This is used for the rest of the logged in session for any other API communications with the server
MASELTOV_USER_PREFERENCES	Holds a JSON Object that includes currently logged in user's preferences
MASELTOV_USER_USERNAME	Holds a string and is the currently logged-in user's username
MASELTOV_USER_ISANONYMOUS	Holds a Boolean (true or false) that denotes if the user is logged in as anonymous (i.e using the anonymous login)
MASELTOV_CHANGE_PASSWORD	Holds a Boolean (true or false) that denotes if the user must be asked to change his/her password

5.2.1.3 Events

As noted in a previous section the user context is captured by a number of MApp applications and is carried as events. Each MApp component sends a number of events to the User Profile, which are subsequently sent to the back-end server and stored for further processing and use by the Recommender system. For communicating events, the User Profile makes available to other MApp applications the User Profile Content Provider (UPCP) to which events are sent. The actual communication of events to the back end server is a sensitive task as the User Profile has to ensure that no information about the user context leaks to potential intruders. Therefore security mechanisms are used for this task. Figure 11 shows the flow of how events are collected from Mapp components and forwarded to the backend server.

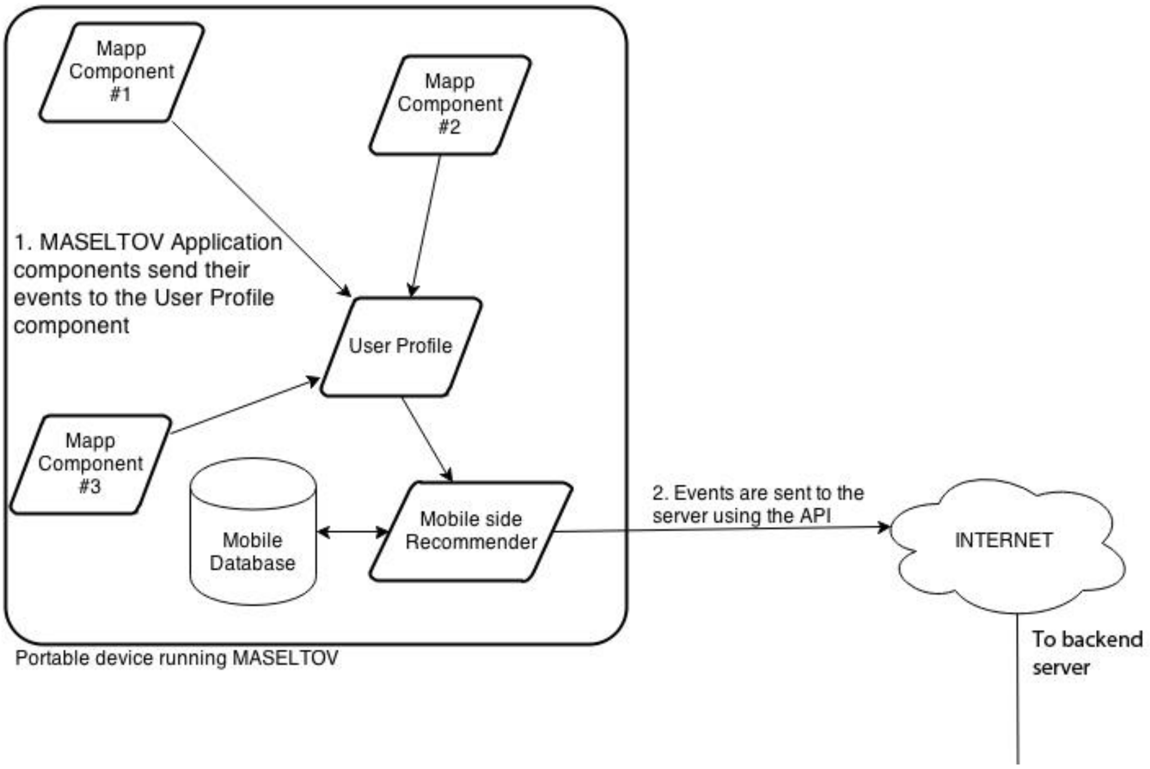

Mapp Component #1
Mapp Component #2
1. MASELTOV Application components send their events to the User Profile component
User Profile
Mapp Component #3
Mobile Database
Mobile side Recommender
2. Events are sent to the server using the API
INTERNET
To backend server
Portable device running MASELTOV

Figure 11: Events collected by UPCP and sent to backend server.

As soon as the UPCP receives an event from a MApp component it stores the data of the event in a local (residing on the smartphone) SQLite database called *MASELTOVEVENTS*. The structure of the database (actually its creation script) is shown in Table 2.

Table 2: SQLite Table events in MASELTOVEVENTS Database.

```
CREATE TABLE `events`
(
 `_ID` INTEGER PRIMARY KEY AUTOINCREMENT,
 `source` VARCHAR(100),
 `timestamp` DATETIME,
 `info` TEXT,
 `locked` INTEGER DEFAULT 0,
 `tries` INTEGER DEFAULT 0
```

```
        )
```

If the device is connected to the Internet the User Profile will attempt to send all pending events to the back-end server using its provided API. The URI used is

http://maseltov.ait.gr/maseltov/wservice/event/<ENCRYPTED_USER_EMAIL>/<PASSWORD_HASH>?timestamp=<EVENT_TIMESTAMP>&id=<EVENT_DB_RECORD_ID>&userid=<USER_ID>&source=<EVENT_SOURCE>&info=<EVENT_INFO_JSON_OBJECT>

where

- *ENCRYPTED_USER_EMAIL* is the user's email encrypted,
- *PASSWORD_HASH* is the user's password hash,
- *EVENT_TIMESTAMP* is the event's timestamp as received by the Mapp component,
- *EVENT_SOURCE* is the event's source as received by the Mapp component,
- *EVENT_INFO_JSON_OBJECT* is the event's info JSON Object that (contains any specific information related to the event) as received by the Mapp component,
- *USER_ID* is the user's id,
- *EVENT_DB_RECORD_ID* is the event's record ID in the local SQLite database used to track the server's response.

The backend server performs an authentication check on the request based on the credentials provided (email and password) and if the user is authenticated the event is recorded in the back-end database.

Failing to record the event will result a failure notice to this API action call and the local SQLite database will retry to send the same event three times. If not successful the whole process terminates.

The *MASELTOVEVENTS* database is used to store the events produced by the MApp components even if the user's device is not connected to the Internet. All events are stored in the database and as soon as the device connects back to the internet those events are transmitted to the back-end server, minimizing the lost information even when the user in not online. The database is dropped when the USER_LOGOUT Broadcast is sent during the Logout procedure.

5.2.1.4 RECOMMENDATIONS

Each user can access and read the personalized recommendations produced for him/her by the Recommender system. The Recommendations component can be accessed from the MApp Dashboard. The client Recommender component retrieves the available recommendations using the following URI of the backend API

http://maseltov.ait.gr/maseltov/wservice /recomm/<ENCRYPTED_USER_EMAIL>/<PASSWORD_HASH>/<NUMBER_OF_ROWS>/<STARTING_FROM>

where

- *ENCRYPTED_USER_EMAIL* is the user's email encrypted,
- *PASSWORD_HASH* is the user's password hash,

- NUMBER_OF_ROWS is the maximum number of recommendation to retrieve,
- STARTING_FROM is the last recommendation's id already received,

The recommendations are also treated securely by the User Profile. As shown above, they are communicated in a way that they are disassociated from the user to whom they are destined. The Recommendations component stores the recommendations locally in an SQLite database called *MASELTOV_RECOMMENDATIONS*. The structure of the database is shown in Table 3.

Table 3: SQLite Table recommendations MASELTOV_RECOMMENDATIONS Database.

```
CREATE TABLE ` recommendations `
(
 `_ID` INTEGER PRIMARY KEY AUTOINCREMENT,
 `id` INTEGER UNIQUE,
 `text` VARCHAR(100),
 `date` VARCHAR(100),
 `time` VARCHAR(100),
 `read` INTEGER DEFAULT 0,
 `star` INTEGER DEFAULT 0,
 `action` VARCHAR(300)
)
```

The backend server performs an authentication check on the request based on the credentials provided (email and password) and if the user is authenticated the list of the recommendations are sent to the device in order to update the local copy of the *MASELTOV_RECOMMENDATIONS* database. This database is dropped when the USER_LOGOUT broadcast is sent during the Logout procedure.

5.3 LOGOUT OPTION

Users can logout from MASELTOV platform by selecting the Logout button under the top right menu in MASELTOV Dashboard. Although this is the easiest and recommended method for a user to logout from the MApp, there are two more cases where the user will lose access to his/her account.

The first case is to explicitly delete all or some of the local data for the MASELTOV application. This can be done if the user selects the Clear Data under the Application Settings → MASELTOV from the Android's main menu. This will delete all application data and the login status will be lost. The user can login again with the same or any other valid MASELTOV account.

The second case is when the user decides to uninstall the MASELTOV application. In this case not only will the application data be lost but the application itself.

In any of the above described methods no user's data are kept on the user's device. Upon a logout all user data are removed. There is no way for a third party to find out from the device who the user that logged in before was or what their preferences were during that session. Moreover, the User Profile uses the Context.sendBroadcast() [3] method to send a broadcast to the other MApp components informing them that the user has logged out so that they stop any services running for this user and remove any data stored locally. This broadcast uses the following action in the Intent.

com.ait.userprofile.USER_LOGOUT

5.4 USER PREFERENCES

User Preferences are received by the backend server during successful login as a JSON object. This consists of a JSON array of JSON objects each one of which holds the field ID and the user's value for that field. An example of a JSON object of user preferences is shown in Appendix B. This JSON object is saved in the variable *MASELTOV_USER_PREFERENCES* using the SharedPreferences Interface as described in Section 5.2.1.2 and in Table 1.

6. USER DATA SECURITY DURING TRANSMISSION

The User Profile uses an API to communicate with the back-end server, so that the User Profile can get user's data saved in the back-end server and also send changed data back to the server. Actions that produce some short of data transmission are listed in Table 4.

Table 4: Actions that transmit data between the device and the server.

Action	Server to Device	Device to Server	Description
Login	√	√	During login, the device sends the user's email and a hash for the entered password and upon successful authentication the server responds with the user's data.
Register		√	During Registration, the device sends the user's data (email, password hash, nickname and city)
Password change		√	When user requests to change their password the device sends to the server the current email and password hash as well as the new password hash.
Event transmission		√	When a Mapp component creates a new event the User Profile sends the event's data to the server (providing user's email and password hash for authentication).
Request recommendations	√	√	When Recommendations component requests for new recommendations the device provides user's email and a password hash. Upon successful authentication the server responds with the data of the new recommendations.
Request usage statistics	√	√	When User Profile requests for usage statistics the device provides user's email and a password hash. Upon successful authentication the server responds with the data of the usage statistics.
Request User Preferences structure		√	Every time the user attempts to log in the User Profile will first request the updated structure of the user preferences. No user-related data are transferred from the server to the device.
Request User Profile categories (drawer list)		√	Every time the user attempts to log in the User Profile will first request the updated list of available categories for the user preferences (the options that are on the User Profile left drawer). No user-related data are transferred from the server to the device.

6.1 HANDLING OF PASSWORDS

6.1.1 REGISTRATION

During registration the user's email is encrypted using the AES algorithm. Upon receiving the encrypted string the server will decrypt it using the same 16-character key used by the User Profile to save the information into the user's table in the database and check if the user already exists. Transmitting the user email as an encrypted string ensures that no eavesdropper who listens to the transmission will be able to recover the user's email address and therefore use it for future attempts, impersonating the genuine user.

During registration, the user is asked to set a password. User passwords are handled by using Lamport's hashes [6]. Actually the server maintains the pair (n, $h^n(p)$), where n is a number that is initialized to a configurable constant N and decremented with each login. The password is hashed with MD5 in order to avoid transmitting the actual password. When the value of n reaches 0 a new password has to be selected and n is set back to N again.

6.1.2 LOGIN

During login the user is asked to enter their email and password. When the User Profile attempts to authenticate the user, it first queries the server for the value of n for the user with the supplied email. The query makes use of the email hashed with MD5. The URI to the API call is

http://maseltov.ait.gr/maseltov/wservice/usern/<HASHED_USER_EMAIL>

to which the server responds (if the user with such an email exists) with the current value of n (it was noted before that each user holds its own value of n). After n is received from the server, user authentication is attempted. The user's email is hashed by the client using MD5 n–1 times and is sent to the server. An attempt to authenticate the user is then performed using the following URI:

http://maseltov.ait.gr/maseltov/wservice
/user/<HASHED_USER_EMAIL>/<PASSWORD_N-1_HASH>

Upon reception of the request the server tries to authenticate the user. It hashes the n–1 hashed password it receives and compares it with the value $h^n(p)$ that it maintains for the user. If the comparison is successful it replaces the pair (n, $h^n(p)$) by (n – 1, $h^{n-1}(p)$). When the value of n reaches 0 a process for selecting a new password is initiated. The user selects a new password, the server stores (N, $h^N(p)$) for the user and the login process resumes.

6.1.3 LAMPORT HASHES

The authentication technique described above is called Lamport hashes. The advantage of the method is that a different hash string is transmitted at every login for a user, therefore it becomes a secure way for authenticating users as it is has no weaknesses for replay attacks. The disadvantage of the method is that $h^n(p)$ must be calculated every time at the client side. Fortunately MD5 is a quick algorithm so the overhead for each login remains low.

6.1.4 FORCE CHANGING PASSWORD

As soon as the n challenge is decremented every time the user performs a successful login, n will reach number 1. Then the User Profile will allow for the last time for the user to login and it will ask for mandatory change of password. As soon as the user enters a new password the value of n will be resumed again to its predefined value (1000 in the case of the current prototype).

7. USER DATA SECURITY IN THE BACKEND SERVER

All user data are saved in a back-end server. For this purpose a MySQL 5.5.32 database is used. User data are saved in two tables, *users* and *user_datafields_values*. The table *users* consist of the fields shown in Table 5.

Table 5: Table users in database.

Field	Description
id	The user's unique ID
user_email	The user's email address. For anonymous registered users the fake email address is stored
user_password	The user's password hash
user_preferences	A JSON Object containing user's preferences. This is used as a caching mechanism in order to serve the user's login requests faster
last_login	The date and time of the last user's successful login
registered	The date and time of the user's registration
n	The current value of the n parameter (the challenge) that is used to create different password hashes every time the user logs in

The table *user_datafields_values* consist of the fields shown in Table 6. This table is used by the recommender to match the user's data with the received events in order to produce the personalized recommendations.

Table 6: Table user_datafields_values.

Field	Description
id	Table's unique ID
user_id	The user's unique ID
field_id	The field's ID
value_id	The value's ID, when the field has specified fields
value	The value, when the field has no specified fields

8. CONCLUSIONS

This document reports on the privacy policy implemented and the security mechanisms used in the context of the MASELTOV platform. It first gives an overview of the existing EU legislation framework and then goes on to explain what policies and how have been implemented in the context of the project. The User Profile is the main component that processes user personal and contextual data, therefore it takes a responsible approach towards their handling. It keeps the user informed about handling of personal data, it allows the user control over what contextual information is allowed to be collected and safeguards their secure communication over the network.

Accompanying processes for handling user data, for example the maintenance of secure backups of user data in the back end server, are not presented in the document. Their implementation is the subject of the MASELTOV service provider.

9. REFERENCES

[1] Android Developer Website, Settings.Security Class, http://developer.android.com/reference/android/provider/Settings.Secure.html

[2] Android Developer Website, Settings.Security Class, ADNROID_ID Constant, http://developer.android.com/reference/android/provider/Settings.Secure.html#ANDROID_ID

[3] Android Developer Website, Context Class, sendBroadcast() Method, http://developer.android.com/reference/android/content/Context.html#sendBroadcast(android.content.Intent, java.lang.String)

[4] Android Developer Website, SharedPreferences Interface, http://developer.android.com/reference/android/content/SharedPreferences.html

[5] Android Developer Website, Context Class, MODE_PRIVATE, http://developer.android.com/reference/android/content/Context.html#MODE_PRIVATE

[6] Password Authentication with Insecure Communication, Leslie Lamport (SRI International), http://research.microsoft.com/en-us/um/people/lamport/pubs/password.pdf

[7] Data Protection Directive 95/46/EC: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm#amendingact

[8] Regulation (EC) No 1882/2003 (Amendment to Data Protection Directive 95/46/EC) http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32003R1882

[9] EC Proposal to reform Data Protection Directive: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[10] Attitudes on Data Protection and Electronic Identity in the EU Barometer Survey 359 (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[11] Ethical Code of Practice_UOC_Draft 1, MASELTV internal document

[12] Progress on Data Protection reform: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_dp_plenary_vote_140312_en.pdf

[13] Lally, V., Sharples, M., Tracey, F., Bertram, N. and Masters, S. (2012). Researching the ethical dimensions of mobile, ubiquitous and immersive technology enhanced learning (MUITEL) in informal settings: a thematic review and dialogue. Interactive Learning Environments, 20(3), pp. 217–238. Available from http://oro.open.ac.uk/33290/1/Interactive_Learning_Environments_Lally_et_al_MUITEL.pdf

[14] http://fc05.deviantart.net/fs71/f/2012/249/d/6/worldwide_photographer__s_rights_by_dougnz-d5bkuez.pdf.

[15] Solove, D.J. (2008) Understanding Privacy, Harvard University Press, London.

[16] Thomas, Keerthi; Bandara, Arosha K.; Price, Blaine A. and Nuseibeh, Bashar (2014). Distilling Privacy. Requirements for Mobile Applications. In: 36th International Conference on Software Engineering (ICSE 2014), 31 May-7 June, 2014, Hyderabad, India (Forthcoming). http://oro.open.ac.uk/

10. APPENDIX A

The following JSON object is a sample that contains the user preferences data structure in English (API action upfields/en/long).

```
{
   "result": {
      "fields": [
         {
            "id": 1,
            "caption": "Username",
            "tag": "TAG_USERNAME",
            "category": "1",
            "mandatory": "1",
            "userEditable": "0",
            "type": "text",
            "description": "This is the username you choose during registration. this username is to protect your identity from the other users.",
            "info": {
               "type": "text",
               "value": "50",
               "tag": "TAG_USERNAME"
            }
         },
         {
            "id": 2,
            "caption": "Email",
            "tag": "TAG_EMAIL",
            "category": "1",
            "mandatory": "1",
            "userEditable": "0",
            "type": "email",
            "description": "this is the user's email and is used a the login username",
            "info": {
               "type": "email",
               "value": "",
               "tag": "TAG_EMAIL"
            }
         },
         {
            "id": 3,
            "caption": "Language",
            "tag": "TAG_LANGUAGE",
            "category": "1",
            "mandatory": "1",
            "userEditable": "1",
            "type": "lang",
            "description": "field description for Language",
            "options": [
               {
                  "id": "6",
                  "caption": "Deutsch",
                  "english_caption": "German",
                  "code": "de",
                  "isactive": "1",
                  "lang_direction": "LTR"
               },
            {
              "id": "1",
              "caption": "English",
              "english_caption": "English",
              "code": "en",
              "isactive": "1",
              "lang_direction": "LTR"
            },
            {
              "id": "4",
              "caption": "Español",
              "english_caption": "Spanish",
              "code": "es",
              "isactive": "1",
              "lang_direction": "LTR"
            },
            {
              "id": "3",
              "caption": "Français",
              "english_caption": "French",
              "code": "fr",
              "isactive": "1",
              "lang_direction": "LTR"
            },
            {
              "id": "5",
              "caption": "Italiano",
              "english_caption": "Italian",
              "code": "it",
              "isactive": "1",
              "lang_direction": "LTR"
            },
            {
              "id": "7",
              "caption": "Türkçe",
              "english_caption": "Turkish",
              "code": "tr",
              "isactive": "1",
              "lang_direction": "LTR"
            },
            {
              "id": "8",
              "caption": "ال عرب ية",
              "english_caption": "Arabic",
              "code": "ar",
              "isactive": "1",
              "lang_direction": "RTL"
            }
          ]
        },
        {
          "id": 4,
          "caption": "Date of Birth",
          "tag": "TAG_DOB",
          "category": "1",
          "mandatory": "0",
          "userEditable": "1",
          "type": "date",
            "description": "This is your date of birth. We use this information in order to calculate your age and
provide you with notifications that we know best fits in people of your age.",
            "info": {
               "type": "date",
               "value": "",
               "tag": "TAG_DOB"
            }
         },
         {
            "id": 5,
            "caption": "Years in Country",
            "tag": "TAG_YEARS_IN_COUNTRY",
            "category": "2",
            "mandatory": "0",
            "userEditable": "1",
            "type": "limit",
            "description": "this defines the nubber of years the user leaves in the country",
            "info": {
               "type": "limit",
               "lower": "0",
               "upper": "50",
               "tag": "TAG_YEARS_IN_COUNTRY"
            }
         },
         {
            "id": 6,
            "caption": "Gender",
            "tag": "TAG_GENDER",
            "category": "1",
            "mandatory": "0",
            "userEditable": "1",
            "type": "enum",
            "description": "field description text for gender",
            "options": [
               {
                  "id": 2,
                  "name": "Female"
               },
               {
                  "id": 18,
                  "name": "Male"
               }
            ]
         },
         {
            "id": 7,
            "caption": "Nationality",
            "tag": "TAG_NATIONALITY",
            "category": "2",
            "mandatory": "0",
            "userEditable": "1",
            "type": "enum",
            "description": "field description text for Nationality",
            "options": [
               {
                  "id": 3,
                  "name": "British"
               },
        {
          "id": 4,
          "name": "German"
        },
        {
          "id": 5,
          "name": "Greek"
        },
        {
          "id": 6,
          "name": "Italian"
        },
        {
          "id": 29,
          "name": "French"
        },
        {
          "id": 30,
          "name": "Spanish"
        }
      ]
    },
    {
      "id": 8,
      "caption": "Education Level",
      "tag": "TAG_EDUCATION",
      "category": "2",
      "mandatory": "0",
      "userEditable": "1",
      "type": "enum",
      "description": "field description text for Education level",
      "options": [
        {
          "id": 7,
          "name": "None"
        },
        {
          "id": 8,
          "name": "Primary School"
        },
        {
          "id": 9,
          "name": "University Degree"
        },
        {
          "id": 10,
          "name": "High School"
        }
      ]
    },
    {
      "id": 17,
      "caption": "Entertainment / Hobbies",
      "tag": "TAG_HOBBIES",
      "category": "2",
      "mandatory": "0",
      "userEditable": "1",
      "type": "menum",
        "description": "field description text for Entertainment/Hobbies",
        "options": [
          {
            "name": "Cooking",
            "children": null,
            "id": 14
          },
          {
            "name": "Games",
            "children": [
              {
                "name": "Adventure",
                "children": null,
                "id": 19
              },
              {
                "name": "Skills",
                "children": null,
                "id": 20
              },
              {
                "name": "Lottery",
                "children": null,
                "id": 21
              }
            ],
            "id": 15
          },
          {
            "name": "Arts",
            "children": [
              {
                "name": "Theatre",
                "children": null,
                "id": 22
              },
              {
                "name": "Cinema",
                "children": null,
                "id": 23
              },
              {
                "name": "Music",
                "children": null,
                "id": 24
              },
              {
                "name": "Museum",
                "children": null,
                "id": 32
              }
            ],
            "id": 16
          },
          {
            "name": "Recreation",
            "children": [
              {
```

```
          "name": "Cycling",
          "children": null,
          "id": 26
        },
        {
          "name": "Running",
          "children": null,
          "id": 27
        },
        {
          "name": "Swimming",
          "children": null,
          "id": 28
        }
      ],
      "id": 25
    }
  ]
},
{
  "id": 19,
  "caption": "Fullname",
  "tag": "TAG_FULLNAME",
  "category": "2",
  "mandatory": "0",
  "userEditable": "1",
  "type": "text",
  "description": "field description text for Fullname",
  "info": {
    "type": "text",
    "value": "60",
    "tag": "TAG_FULLNAME"
  }
},
{
  "id": 20,
  "caption": "Current job",
  "tag": "TAG_CURRENT_JOB",
  "category": "2",
  "mandatory": "0",
  "userEditable": "1",
  "type": "text",
  "description": "field description text for Current Job",
  "info": {
    "type": "text",
    "value": "60",
    "tag": "TAG_CURRENT_JOB"
  }
},
{
  "id": 21,
  "caption": "Religion",
  "tag": "TAG_RELIGION",
  "category": "2",
  "mandatory": "0",
  "userEditable": "1",
  "type": "text",
  "description": "field description for Religion",
          "info": {
            "type": "text",
            "value": 50,
            "tag": "TAG_RELIGION"
          }
        },
        {
          "id": 23,
          "caption": "GPS Tracking",
          "tag": "TAG_GPS_TRACKING",
          "category": "3",
          "mandatory": "0",
          "userEditable": "1",
          "type": "switch",
          "description": "Enables tracking of your position in order to notify you about Points of interest near you, based on your preferences",
          "info": {
            "type": "enum",
            "value": "33;34",
            "tag": "TAG_GPS_TRACKING"
          }
        },
        {
          "id": 24,
          "caption": "Language skills",
          "tag": "TAG_LANGUAGE_SKILLS",
          "category": "5",
          "mandatory": "0",
          "userEditable": "0",
          "type": "menumint",
          "description": "field description text for Learning Skills",
          "options": [
            {
              "name": "English",
              "children": [
                {
                  "name": "Reading",
                  "children": null,
                  "id": 36,
                  "value": ""
                },
                {
                  "name": "Writting",
                  "children": null,
                  "id": 37,
                  "value": ""
                },
                {
                  "name": "Listening",
                  "children": null,
                  "id": 38,
                  "value": ""
                },
                {
                  "name": "Speaking",
                  "children": null,
                  "id": 39,
                  "value": ""
            }
          ],
          "id": 35
        },
        {
          "name": "Spanish",
          "children": [
            {
              "name": "Reading",
              "children": null,
              "id": 41,
              "value": ""
            },
            {
              "name": "Writting",
              "children": null,
              "id": 42,
              "value": ""
            },
            {
              "name": "Listening",
              "children": null,
              "id": 43,
              "value": ""
            },
            {
              "name": "Speaking",
              "children": null,
              "id": 44,
              "value": ""
            }
          ],
          "id": 40
        },
        {
          "name": "German",
          "children": [
            {
              "name": "Reading",
              "children": null,
              "id": 57,
              "value": ""
            },
            {
              "name": "Writting",
              "children": null,
              "id": 58,
              "value": ""
            },
            {
              "name": "Listening",
              "children": null,
              "id": 59,
              "value": ""
            },
            {
              "name": "Speaking",
              "children": null,
               "id": 60,
               "value": ""
            }
         ],
         "id": 56
      }
   ]
},
{
   "id": 25,
   "caption": "City",
   "tag": "TAG_CITY",
   "category": "1",
   "mandatory": "1",
   "userEditable": "1",
   "type": "enum",
   "description": "field description text for City",
   "options": [
      {
         "id": 45,
         "name": "London"
      },
      {
         "id": 46,
         "name": "Madrid"
      },
      {
         "id": 47,
         "name": "Vienna"
      }
   ]
},
{
   "id": 26,
   "caption": "Activity Recognition",
   "tag": "TAG_ACTIVITY_RECOGNITION",
   "category": "3",
   "mandatory": "0",
   "userEditable": "1",
   "type": "switch",
   "description": "Detects the optimal timing for recommendations.",
   "info": {
      "type": "enum",
      "value": "48;49",
      "tag": "TAG_ACTIVITY_RECOGNITION"
   }
},
{
   "id": 27,
   "caption": "Interest Sensing",
   "tag": "TAG_INTERESTS_SENSING",
   "category": "3",
   "mandatory": "0",
   "userEditable": "1",
   "type": "switch",
   "description": "Helps to deliver highly personalized recommendations.",
   "info": {
      "type": "enum",
                "value": "50;51",
                "tag": "TAG_INTERESTS_SENSING"
            }
        },
        {
            "id": 28,
            "caption": "Semantic Place Detection",
            "tag": "TAG_PLACE_DETECTION",
            "category": "3",
            "mandatory": "0",
            "userEditable": "1",
            "type": "switch",
            "description": "Enables daily reflection on places visited as well as recommendations for places.",
            "info": {
                "type": "enum",
                "value": "52;53",
                "tag": "TAG_PLACE_DETECTION"
            }
        },
        {
            "id": 29,
            "caption": "Social Interaction",
            "tag": "TAG_SOCIAL_INTERACTION",
            "category": "3",
            "mandatory": "0",
            "userEditable": "1",
            "type": "switch",
            "description": "Supports and facilitates social inclusion.",
            "info": {
                "type": "enum",
                "value": "54;55",
                "tag": "TAG_SOCIAL_INTERACTION"
            }
        },
        {
            "id": 30,
            "caption": "Coins",
            "tag": "TAG_COINS",
            "category": "5",
            "mandatory": "0",
            "userEditable": "0",
            "type": "num",
            "description": "This shows the current number of coins the user holds to be redeemed within the
application",
            "info": {
                "type": "num",
                "value": "",
                "tag": "TAG_COINS"
            }
        },
        {
            "id": 31,
            "caption": "Help Radar Volunteer Code",
            "tag": "TAG_VALIDATION_CODE",
            "category": "1",
            "mandatory": "0",
            "userEditable": "1",
            "type": "text",
                "description": "Add your volunteer code in this field to certify that you are a registered and approved
volunteer",
                "info": {
                    "type": "text",
                    "value": "50",
                    "tag": "TAG_VALIDATION_CODE"
                }
            }
        ]
    }
}
```

11. APPENDIX B

The following JSON object sample contains the user's preferences and is returned from the server to the device after a successful login.

```
{
  "result": {
    "user": {
      "id": 7,
      "useremail": "2f59747435312e44cd8ca3e1f1e7d6bd",
      "username": "geoak79",
      "preferences": [
        {
          "id": "1",
          "value": "geoak79"
        },
        {
          "id": "2",
          "value": "iage@ait.gr"
        },
        {
          "id": "3",
          "value": "{\"id\":\"1\"}"
        },
        {
          "id": "6",
          "value": "{\"id\":\"18\"}"
        },
        {
          "id": "17",
          "value": "[{\"id\":\"14\"},{\"id\":\"20\"},{\"id\":\"22\"},{\"id\":\"23\"},{\"id\":\"32\"},{\"id\":\"26\"},{\"id\":\"27\"},{\"id\":\"28\"}]"
        },
        {
          "id": 7,
          "value": "{\"id\":\"5\"}"
        },
        {
          "id": 19,
          "value": "Iakovos"
        },
        {
          "id": 8,
          "value": "{\"id\":\"9\"}"
        },
        {
          "id": 4,
          "value": "19790710"
        },
        {
          "id": 23,
          "value": "1"
        },
        {
          "id": 24,
          "value": "[{\"id\":\"36\",\"value\":\"3\"},{\"id\":\"37\",\"value\":\"1\"}]"
        },
        {
          "id": 20,
          "value": "Researcher"
        },
        {
          "id": 21,
          "value": ""
        },
        {
          "id": 25,
          "value": "{\"id\":\"45\"}"
        },
        {
          "id": 26,
          "value": "1"
        },
        {
          "id": 27,
          "value": "0"
        },
        {
          "id": 28,
          "value": "1"
        },
        {
          "id": 29,
          "value": "0"
        },
        {
          "id": 5,
          "value": "34"
        },
                {
                    "id": 30,
                    "value": "120"
                },
                {
                    "id": 31,
                    "value": "ABCDEFG123"
                },
                {
                    "id": 32,
                    "value": "1"
                }
            ]
        }
    }
}
```