eVACUATE

FP7-313161

A holistic, scenario-independent, situation-awareness and guidance system for sustaining the Active Evacuation Route for large crowds

ETHICAL AND LEGAL REQUIREMENTS ANALYSIS (SPECIFICATIONS, PROPORTIONALITY, IMPLEMENTATION AND EVALUATION)

Deliverable Identifier:	D.11.3
Delivery Date:	Mar 31, 2016
Classification:	Public
Editor(s):	Diana Dimitrova (KUL);
Document version:	1.0 - 2016
Contract Start Date:	April 1st, 2013
Duration:	48 months
Project coordinator:	EXODUS S.A. (Greece)
Partners:	EXO (GR), IT INNOVATION (UK), ICCS (GR), HKV (NL), TEL (GR), TEK (ES), AIA (GR), VITRO (IT), CDI (UK), INDRA (ES), KUL (BE), DXT (FR), POLITO (IT), STX-FR (FR), TUD (DE), TUC (DE), ASRS (ES), METB (ES), TIM (IT)

Project co-funded by the European Commission under the 7th Framework Programme

SEVENTH FRAMEWORK PROGRAMME

Document control page

Title	**Ethical and legal requirements analysis (specifications, proportionality, implementation and evaluation)**	
Editors	Diana Dimitrova	KUL
Contributors	Diego Betancourt	TUD
	Dimitris Drakoulis	TELESTO
Peer Reviewers	Eduardo Martinez Gil	INDRA
	Hanneke Vreugdenhil	HKV
Format	Text - Ms Word	
Language	en-UK	
Work-Package	WP 11	
Deliverable number	D.11.3	
Due Date of Delivery	31/03/2016	
Actual Date of Delivery	31/03/2016	
Dissemination Level	One of the following: Public Restricted to other programme participants (including the Commission Services) Restricted to a group specified by the consortium (including the Commission Services) Confidential, only for members of the consortium (including the Commission Services)	
Rights	eVACUATE Consortium	
Audience	☒ public ☐ restricted ☐ internal	
Date	31/03/2016	
Revision	none	
Version	1.0	
Edited by	Diana Dimitrova	
Status	☐ draft ☒ Consortium reviewed ☒ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	04/03/2016	Comments and corrections provided by HKV	Hanneke Vreugdenhil
0.2	07/03/2016	Integration of HKV comments	Diana Dimitrova
0.3	08/03/2016	Revisions by INDRA	Eduardo Martinez Gil
1.0	31/03/2016	Final version- Ready for submission	Dimitris Petrantonakis

Table of Contents

Table of Figures

Executive summary

The present deliverable builds on the Ethical and Legal requirements analysis of D11.2. The major thrust of D11.2 was the privacy, data protection and ethical issues in eVACUATE. It focused on (1) the different elements of the eVACUATE solution, i.e. the individual technologies (chipless RFID tags, eVAMAPP, Social networks datamining, crowd behaviour detection through video surveillance) as well as (2) on the four validation demonstration scenarios, especially through the proportionality perspective, and related to that – the eVACUATE solution as a whole.

The purpose of D11.3 is to report the latest analysis of and recommendation given to the individual technologies from an ethical, privacy and data protection perspective. This analysis is helpful not only in the technical development of the eVACUATE solution in itself within the eVACUATE project. This ethical and legal recommendations could also be used in the operational deployment of eVACUATE or individual components thereof and in the development of similar technological solutions beyond the eVACUATE project.

The current deliverable is structured as follows:

After the introduction, **Chapter 2** focuses on the analysis of the individual elements of the eVACUATE solution. It starts by providing additional remarks to the Privacy Impact Assessment **(PIA)** of the **chipless RFID tags**. Its main conclusion is that while there are remaining issues concerning the full privacy compliance of the technology, there has been progress made with regards to the individual privacy and data protection recommendations.

The deliverable then goes on to discuss the **eVAMAPP** and the Social Networks manager **(SoNeMa)**. The main issues discussed concern the *necessity and proportionality* of some of their features, especially because of their personal data processing features. Relevant examples are checking and monitoring over time the influence scores (KLOUT scores) of individual Twitter users (SoNeMa) or the method of identifying and monitoring the location of eVAMAPP users. Another aspect is the proper *legal basis* for collecting personal data via social networks, whether and how it could be collected without the consent of social network users. Ethical issues are also addressed, e.g. collecting and providing too much information to first responders, who might be overwhelmed by unnecessary information.

The discussion ends with further remarks on the **crowd behaviour detection video surveillance technology**. It addresses the risks related to the analysis of soft biometrics, e.g. crowd's or individuals' behaviour and gait. It focuses on the risks which the technology poses for the identifiability and privacy of individuals, even when the focus of the behaviour analysis is the crowd.

As to **proportionality**, in D11.2 a separate chapter was devoted to the proportionality analysis, carried out through analysing the scenarios for the validation demonstrations. In the present deliverable, remarks regarding the proportionality of the solution and the scenarios are integrated into the discussion of the technologies. Thus, the questions of the actual *necessity and proportionality* of certain features of the eVACUATE solution in the context of emergency response are being tackled.

1. Introduction

In the past months the different technological elements of the eVACUATE solution have been further developed to be brought to their final shape. The further details of the technologies and the clarifications about their purposes and functionalities brought to the fore additional privacy, data protection and ethical issues that needed to be addressed. The discussion and recommendations that will follow in the chapters below are a continuation of the analysis made in D11.2. The present deliverable will thus focus on the following issues:

1) How have the data protection and privacy risks of the **chipless RFID application** been addressed so far and what further recommendations should be taken into account? This is in effect an elaboration on the first version of the Privacy Impact Assessment (PIA).
2) What are the additional ethical, data protection and privacy concerns that need to be addressed with regards to the different **smartphone apps**, developed in the framework of eVACUATE? The focus has been especially on the issues of the identification of individuals through these apps, their location information and possibly further personal data, the proper storage place and storage period for this data, as well as defining the legitimate usage of the apps.
3) What are the privacy, data protection and ethical risks that **SoNeMa** poses and how can they be mitigated? The analysis includes a discussion of the possible legal basis for mining social networks in general, the privacy-friendly usage of SoNeMa, its legitimate use and relevance of the SoNeMa features in the emergency management context.
4) What are the risks of identifying individuals through **crowd behaviour monitoring technologies** and what are the privacy risks to individuals even if they remain anonymous within the crowd?

In analysing the above risks and answering the questions posed above relevant examples have been drawn from the eVACUATE scenarios as described in December 2015. The discussion also involves an assessment of the *necessity and proportionality* of the elements of the eVACUATE solution and its possible operation on an uninterrupted basis in operational situations.

Issues related to the privacy and data protection compliance of the project during the validation demonstrations and research activities are currently being addressed within the project. The work done towards this end will be reported in D11.5, which will be submitted at the end of the project at M50. D11.5 will contain additional remarks to the elements of the eVACUATE solution from an ethical, privacy and data protection perspective, if any need to be made, e.g. as a result of insights of the impact of the technology on individuals' rights to privacy and data protection when the technologies are being demonstrated during the validation demonstrations.

2. Comments to the eVACUATE technologies

2.1. RFID chipless tags

2.1.1. Update of the technology

The further work carried out in the past months on the chipless RFID tags in WP7 has been explained in eVACUATE deliverable D7.7. From this report it has become clear that the role of these tags will be to update and maintain the Active Evacuation Route (AER) by counting the number and type of individuals who pass through a specific place, where an appropriate RFID reader is installed, e.g. at the entrance of a metro station. This technology, however, does not show the direction of movement of the individuals, i.e. it can only locate the proximity of a certain tag next to an RFID reader, without knowing whether actually someone has exited the space and should not be counted as part of the crowd any more.[1]

Amongst the many aspects of the technology, D7.7 points out certain practical issues that could result in the decrease of the accuracy of the technology. This could happen (1) when the tags are held by human beings as the human body can block the signal as a result of which the specific person is not being detected (i.e. the human body as a factor), (2) bending and folding of the tags, and (3) the tag's reading range of only 1m. In addition, the eVACUATE RFID technology cannot determine the direction of movement, e.g. whether people are entering or exiting a place. It can only determine the proximity of a tag to a reader.

2.1.2. Data protection, privacy and ethical issues

Chapter 3 of D11.2 provided a first overview of the Privacy Impact Assessment (PIA) that needs to be carried out for RFID tags. As a recap, the purpose of the PIA is to identify the privacy and data protection risks associated with the RFID application, as well as to define the mitigation measures that need to be taken in respect of these risks. This is to help the operators of RFID technologies be privacy compliant and monitor more systematically their privacy compliance throughout the period of operation of their RFID technology.

The table below (Figure 1) re-captures the privacy and data protection risks already identified in D11.2. In the second column it discusses the mitigation measures that have been recommended and/or already implemented and adds proposals for additional mitigation measures.

It is reminded here that the tags are not individualized, e.g. they do not contain names or other unique identifiers. However, they could contain information about the individual who carries them. This information could be sensitive, e.g. that someone is pregnant or has a disability. This could make it possible to single out certain individuals and track these through the chipless RFID technology. A relevant example of singling out individuals would be if there is only one disabled person at particular point in time that has a ticket marked as "disabled." Thus, every time the chip is read, it could be known where this particular individual is located. This can be enhanced by a combination of the information from the RFID technology and the video surveillance technology, for

[1] Diego Betancourt's (TUD) email from 16.11.2015

instance. Thus, there is the possibility for singling out and possibly identifying individuals.

The purpose of the table below is to report on how in the past months measures have been taken to mitigate the identified risks. If measures have not been taken or implemented yet, the table provides detailed suggestions of what measures need to be implemented. In principle, the risks and mitigation measures as elaborated on below apply to both the validation demonstrations within the framework of eVACUATE and to the potential future usage of the technology in operational situations. However, it is acknowledged that the mitigation measures in operational situations could be nuanced from the ones during research due to the different level of the risks posed by research and by the operational exploitation of the technology. For example, when appropriate storage periods for the location of tags at certain moments are being determined, then these storage periods will differ for the research case and the operational case, as the purpose of the usage of the technology in those two cases differ and sometimes longer data storage for research purposes is allowed.

	Risk	Explanation/Mitigation measure
1.	Information security (e.g. skimming, eavesdropping)	The risk for the individuals carrying the tickets is that their location may be tracked by those who have illegitimate access to the tag and who may also access the information on the tag, e.g. that a woman is pregnant or that someone is disabled. Another risk is that the communication between the reader and the tag is eavesdropped and again unauthorized people could obtain information about the individuals and their movements. As the chipless RFID technology is part of the overall eVACUATE solution, the adequate security measures that concern the chipless RFID technology should be considered in the overall security design of eVACUATE. D6.3 has dealt with the issue of security of the eVACUATE solution, including security of the RFID application. Ongoing
2.	Information accuracy (info on ticket and of number of people), e.g. when ticket bent or carried by people	Accuracy is essential for obtaining a reliable situation on the number of persons in a certain area. In 2015 further research has been undertaken by TUD and TUC to explore the technical issues related to the accuracy of the technology. The scientific work done towards this end has been reported in D7.7. Ongoing
3.	Lack of transparency	It is essential that the individuals who will use the technology are being informed about the purposes and the usage of the technology, as well as relevant details about the data processing by the technology, the voluntary nature of the usage, as well as the identity of the controller. The information notice should be drafted in a manner understandable to the common individuals and should be tailored for the specific case. Thus, before the four validation demonstrations, KUL will provide assistance to the end-users about the relevant consent form and information notice to be

		given to the volunteers. As to the operational environment, the proposed forms for the validation demos should be adjusted by the end-users and can thus serve as templates. Ongoing
4.	Lack of voluntariness	Those individuals who will use the technology should do so on a purely voluntary basis. This means that no one should be forced to purchase tickets or cards that contain the RFID tag, either during the demos or in operational situations. Individuals should be *explicitly informed* that their usage of the technology is voluntary and no negative consequences will ensue if they do not wish to use it. If tickets are purchased from machines, individuals could be given the opportunity to press an "I agree button" after they have read the consent form and information notice in order to proceed with the purchase of a tagged ticket. As to the validation demonstrations more specifically, it is planned that there will be a consent form for the volunteers who will participate in these demos and this consent form should encompass the usage of RFID tickets during the validation demonstrations. These forms will be prepared and tailored for each demo in the course of the preparations for the demo in the months preceding the demos. Ongoing
5.	Re-use of data (e.g. information that someone is disabled) for incompatible purposes (e.g. marketing, tracking not related to evacuation and crowd management purposes)	This risk can be mitigated through clear policies and commitments by the individuals who have access to the data. Thus, one needs to have a clear and strict policy on access control to the data and ensure against the re-use of the data. For the eVACUATE validation demonstrations, there will be a clear recommendations not to use the data for other purposes than research purposes in eVACUATE and to delete the data at the end of the project at latest. In an operational environment each end-user should have a clear data access and usage policy, which specifies a limited number of individuals who have access to the data and who should be

		instructed to use the data only for purposes of counting individuals and their categories, as well as their approximate location. Ongoing
6.	Data storage and tracking	In principle personal data needs to be deleted as soon as it is not necessary any more for the purposes for which it is being processed. The risk is that if data is stored over a long period of time, the movements of particular people could be reconstructed. One example how this could happen is if at a certain time there is only one individual who belongs to a particular category, e.g. disabled, and the movements of this person are re-constructed over time and space. Since this would not be necessary for the purpose of evacuation, e.g. data from the previous week, then such situations should be prevented through proper deletion policies. In the case of RFID tags, for the research case, the data will be deleted at the end of the project at latest, i.e. shortly after the end of the validation demonstrations. The partners will be instructed not to use the data for other purposes that the research purposes as set out in eVACUATE. Completely anonymized data, e.g. statistical data, may be retained for longer when they do not represent privacy or data protection risks. The challenge is to find an adequate deletion and no-tracking policy for operational situations. The RFID technology cannot determine the direction of movement and the tags are not individualized. Thus, the technology cannot determine whether a certain individual is still inside or outside the premises and thus delete their individual records from the eVACUATE solution once these people are outside the end-user premises. A possible solution would be deleting all records at regular intervals, which should be determined by each end-user on a case-by-case basis. Ongoing
7.	Data combination (of RFID data with other data such as CCTV)	The risk is that such a combination increases the identifiability of individuals. Thus, it is essential that if the information between those two technologies is cross-linked, solution can be found that

	the interlinkage takes place once an emergency is declared and the data would be necessary for the emergency response and saving human life. Ongoing

Figure 1: eVACUATE Chipless RFID technology risks and mitigation measures (PIA)

2.1.3. Summary of recommendations and conclusions

The discussion reveals that while the eVACUATE chipless RFID technology does not as such seek to identify individuals, it still poses certain risks to their privacy and data protection rights. Thus, in the further development of the technology and its potential future exploitation in operational situations, the risks discussed above should be addressed in order to prevent the negative impact on individuals.

The recommendations made in D11.2 continue to apply. Below is a summary of these recommendations and in how far they have been taken into account in the development of the technology do far. Action points have been added for the recommendations that still need to be fulfilled:

1. The purposes of the RFID technology for the eVACUATE scenarios have been more narrowly defined in D7.7. It is important that the actual performance of the technology can support the reliable fulfilment of those purposes. In operational cases, each future operator (end-user) should also clearly define the purposes for which they intend to introduce the RFID technology (in case they are even slightly different from the ones explained in D7.7) and not use the personal data processed through it for further, incompatible purposes.
2. Purchasing tickets that contain the eVACUATE chipless RFID tag should be voluntary. This means that the operation of the RFID technology should be based on the consent on the individuals who will carry the tags (Article 7 (a) Directive 95/46/EC). This applies both to the case of the validation demonstrations in eVACUATE and to the operational exploitation of the technology. If the consent is given explicitly (example be being to choose between clicking on an “I agree button” vs. “I do not agree” button), then it will be easier for the controller[2] of the technology to prove that the usage of the technology is consensual.
3. Before consent is granted by the concerned individuals, sufficient and understandable information about the purposes of the RFID technology, the data processed through it, the voluntary nature of participating in it, as well as the possible sharing of this data should be provided. **The respective information notice and consent as part of the eVACUATE scenarios will be drafted for the validation demonstration(s) by KUL. It can be used also as a template for future operational scenarios.**
4. Data security should be guaranteed at all times.
5. The issue of the accuracy of the data processed, e.g. due to the bending of tags, their interaction with the human body, should be improved. **TUD is continuing to work in that direction.**
6. A proper deletion policy should be determined. For the validation demonstrations the latest deletion should be the end of the project. For operations cases, it is suggested that the data is deleted every 30 minutes to 1 or 2 hours. This is to be determined by every end-user depending on the use-case. For the declared purposes of the eVACUATE project it appears that only the latest reading from a reader will suffice.

[2] Controller here is used in the data protection sense of the word, see Article 2 (d) Directive 95/46/EC.

2.2. The eVACUATE Mobile Application (eVAMAPP)

The following analysis of the eVACUATE Mobile Application Framework (in short we refer to it as "eVAMAPP") builds on the initial analysis made in D11.2, where specific recommendations about the design and operation of the eVAMAPP were offered. These are summarized below, Section 2.2.1. Afterwards the chapter continues with additional recommendations, since in the past months the eVAMAPP has been further developed and elaborated on, with some of its features becoming much clearer. Thus, such additional elements concerning the app need to be analysed from an ethical and privacy and data protection perspective.

It has become clear that in the eVACUATE project four different types of apps are being developed and tested, and their features have been elaborated on in more detail in the past months:

(1) An app specifically dedicated to passengers to help them evacuate, e.g. from the cruise ship.
(2) An app dedicated specifically to cruise crew members who are in charge of the mustering at cruise ships. It is aimed at helping the crew members find out who is missing and has not mustered (the "missing people" app).
(3) An app dedicated to first responders in general to help them manage alerts (the "First Responders App).
(4) An app for generic use by facility visitors that will support the other proof-of-concept scenarios (generically), i.e. the "airport scenario", the "stadium scenario" (the "metro" scenario does not represent a case where people stand to benefit from the use of a mobile app).

D11.2. examined the features of the first app, as they were being presented at the time of writing of D11.2. Also, certain legal aspects about the app for personnel/crew members were pointed out. Due to the further developments of all the apps, the present deliverable will focus on these new elements and provide recommendations. The main focus will be on the purpose limitation, i.e. setting out more clearly the purposes of each app, as well as the details of the data processing, especially linking a certain location to a specific individual and preventing general and constant tracking of all individuals who have downloaded the app.

2.2.1. App for common people/cruise ship passengers

As a recap from D11.2, the deliverable contained the following analysis and recommendations:

- It is essential to establish clearly the purpose of the usage of each app, which is important for defining the legal usage of the app and preventing against arbitrariness, such as illegal re-use of the data.
- Setting out clear data deletion periods to avoid storage of data for longer than necessary, e.g. storing all location information of a certain app user, which enables their tracking all the time.
- Compliance with the data minimization principle, i.e. not processing more data than necessary for the purposes of the specific app.

- Necessity for providing adequate information to the individuals before downloading the app and giving them the opportunity to give their *free, specific and informed consent*.
- Recommendation was made on the appropriate legal basis, i.e. consent which satisfies 95/46 and the e-Privacy Directive. This legal basis is especially relevant for the validation demonstrations. Article 7 (d) Directive 95/46 EC as an alternative legal basis for those who withdraw their consent was also considered.
- The privacy and data protection issues related to location tracking through the app were studied, as well as sending audio-visual information through the app to the crew personnel. Additional aspects of the analysis were logging of transaction data, sensing and sending environmental information of those who report themselves sick, ensuring data security throughout the whole data processing cycle, and liability issues the for survival kit content.

2.2.1.1. Further elements of the eVAMAPP for passengers

From the information provided by TELESTO, it is understood that the **purposes** of the cruise ship passenger app are to provide safety and evacuation information, as well as the Active Evacuation Route (AER) to the passengers and help first responders find their location in those cases when someone is declared missing or not moving. Thus, it is welcome that the purposes of the usage of the app have been more narrowly defined in the past months.

A crucial detail concerning the functioning of the app and its ability to **track the location of the devices** on which the app is downloaded, is how the passengers, who will be app users, will be identified by/through the app and how their location will be tracked through the eVAMAPP. More concretely, the question concerns how the link between *the device, the identity of the individual and his/her location* will be established, and then *communicated* to the eVACUATE solution, both during the validation demonstration and subsequently, in operational cases.

As explained by TELESTO, for the case of the *validation demonstrations*, to test the eVAMAPP, a private WiFi network will be set up by the eVACUATE partner Telecom Italia (TIM). When someone, i.e. a volunteer for the demos, wants to download the app, they will have to register both for the private WiFi and the eVAMAPP. The private WiFi will be able to see all the MAC addresses of any device that is found in the area/field of the private WiFi and which has the WiFi switched on. A person's identification for the WiFi will happen via the MAC address of their terminal device and the WiFi registration details, such as the user ID (the user ID and password are necessary for logging in to the WiFi). [3] However, the WiFi will be able to see the MAC addresses of everyone passing by, including people who are not volunteers and who have not given their consent. Since in many EU countries its IP addresses, especially static IP addresses such as MAC addresses are considered to be personal data, in eVACUATE it is also recommendable to treat these addresses as personal data.[4] The SABAM case

[3] Telco with TELESTO, 5 November 2015

[4] Time.lex, "Study of case law on the circumstances in which IP addresses are considered personal data, D3. Final Report," SMART 2010/12. 2 May 2011

of the European Court of Justice classified IP addresses since "they allow the users to be precisely identified."[5] In eVACUATE the MAC addresses of the volunteers will be processed. Volunteers will have to register in the private WiFi as explained above. Thus, their identities will be known. However, the WiFi technology in eVACUATE could also see the MAC addresses of any passer-by. If one assumes that MAC addresses are static and by crosslinking the MAC addresses with other identifiable information, even if this information is not immediately available to the TIM, TIM may be able to identify individuals, then it is safer to treat the MAC addresses as personal data. Moreover, since a lot of the MAC addresses will not belong to volunteers for the demos, it is recommended that the MAC addresses are immediately deleted.

As to those who will download the app, as explained by TELESTO, in eVACUATE the location of persons who have downloaded the eVAMAPP will be obtained through Bluetooth tracking, whereby the Bluetooth antennas, which would be installed at different points on the ceiling of the ship and through which a passenger passes, will collect the location info of the device. The Bluetooth on the smartphone using the eVAMAPP can be switched on already when someone downloads and starts the app. The EOC will obtain the location data of the devices with the eVAMAPP only if an emergency is declared by the authority/individual who is authorized to declare such emergencies, even if the Bluetooth of an app is switched on before that. In addition, when an emergency is declared, the apps will get the message that there is an emergency and the Bluetooth must be manually switched on.[6] Thus, if an app has its Bluetooth active all the time, the antennas will collect the location information. This location information, linked to the device and to the identity of the person holding the device, will be stored on the private WiFi network, manufactured by Telecom Italia's subcontractor the MobiMESH.[7] A person's identification information can be used later, in emergency cases if someone has not mustered, to link the location of a certain device to the owner of the device and possibly locate the missing person on the basis of this information. In addition, the eVAMAPP could detect whether someone is moving or has stopped or even fallen by looking at the acceleration of the movement of the device.

2.2.1.2. Legal and ethical recommendations

When the further technical details are being considered in the design of the eVAMAPP and the overall technical solution, it is recommended, pursuant to the purpose limitation and data minimization principles, that the registration of personal data provided by the passengers is only the minimum necessary to establish their identity, e.g. name and location to be able to actually help them evacuate when needed. Thus, when downloading the app, the passengers, after having read the information about the app and the personal data to be processed by it and having given their *free, specific and informed* consent, could provide, e.g. again only their names (e.g. in the registration to the private WiFi, in which also the MAC address is known). If somebody is declared missing (not having reached the mustering station), the mustering personnel will see their names on the list of missing people. An automated search with the name could

[5] Court of Justice of the European Union, *SABAM,* C – 70/10, 24 November 2011, Par. 51
[6] Email from TELESTO, 8 December 2015
[7] Telco with TELESTO, 5 November 2015

be carried out, i.e. searching the records of the locations of the devices which have downloaded the app with the name of the missing person.

Related to the personally identifiable information for the app, including the information on someone's location, is the question of **data storage** and **data access** once it is collected by Bluetooth. It is positive that the identity and location of a person are accessible to the responsible personnel (e.g. via the Emergency Operational Centre (EOC)) only if someone is declared missing and they need to be located to be rescued. Here, it is recommendable that while the EOC has access to the identity and location data of the app users when they need to search for someone, if the emergency is not such as to result in missing individuals, then the EOC should not access this data. This is to avoid the generalized tracking of all app users, the majority of which is hoped to be able to evacuate safely without the need for an special assistance based on their being localized through the app. After the emergency, when everyone has mustered, this information should be deleted as it would not be necessary any more. An additional data protection measure is storing only the last known location to avoid permanent tracking of the eVAMAPP users. As explained above, since the location of individuals will be stored on the private WiFi network, it is recommendable that also the WiFi does not store all the location info, but only the last one or two or up to three known locations. It is recommendable also the additional personal information, known to the WiFi, such as MAC address and name, are not connected to other available information on the individuals. For example, in the cruise ship case, the passengers' names are stored on the FIDELIO database, together with further personal information, such as their cabin number, credit card number, disability information if available, etc. This opportunity to link a device to a person and obtain additional personal data about them makes it even more crucial that the devices are not tracked all the time and the data from the WiFi are not cross-linked with other personal data, unless someone is declared missing and has to be located and rescued. Last but not least, the access to the personal information stored on the private WiFi needs to be controlled too, in order to avoid illegal access to the data of individuals and their tracking. In this respect, also proper data security and access measures need to be taken.

As to the detection of falling or movement (and lack thereof), it is indicated in the cruise ship scenario (timestamp 5.30) that the eVAMAPP will be used to detect a disabled person who has stopped moving. In this case, the app is used not to find a missing person, but to assist a person who might possibly not be able to evacuate himself. As the evacuation will already be declared, the EOC will receive the location data obtained through the app. While it is recommended to avoid generalized tracking, if the feature is adapted to only detect a certain location around which the acceleration of the device has dropped to zero (without further personal details such as the name of the person), i.e. it is anonymized, then the privacy risks will be lower. It is important to know, however, that it is possible that a mobile device actually falls off in the process of evacuation, especially in crowded environments. In such cases, the 0 acceleration might simply mean that the device has fallen, while its owner has continued successfully evacuating. Such misleading information should not lead to stretching the human resources available, as this would act in a way as a false alarm.

Last but not least, there are also some ethical remarks that should be made with regards to the usage of the eVAMAPP. In principle, as technologies are not free from flaws, sometimes the information collected or provided by them is not accurate. Therefore, first responders should avoid overreliance on the information provided by such apps, e.g. as to the possible location of a missing person, and have available other means of finding and assisting missing individuals. The tests and the validation demonstrations could be used as an opportunity to test the reliability of device location to check in how far the location information is accurate. This would contribute also to the *legal assessment of whether the eVAMAPP would be necessary and proportionate* response to the purposes it pursues, especially its purpose to track individuals who are missing by collecting their location data.

Related to this is also the possible digital divide that such an eVAMAPP could lead to. An illustrative example would be if two people are declared missing and one of them has downloaded the app and the other one has not. In both cases human life is at stake and therefore equal efforts should be spent on locating and saving both individuals, without prioritizing the one who uses the app.

2.2.2. App for first responders

It has been decided that in the eVACUATE project there will also be an app for the first responders, whose **purpose** will be to manage the alerts more efficiently and enable the communication between the first responders about the actions taken with regards to a certain alert.

The benefits of such an app for a timelier and better coordinated emergency response are very welcome. While its operation could significantly improve the work of first responders, still the data protection recommendations should be fully respected. As explained in more detail in D11.2, the operation of such an app would take place in the employment context. As to the legal basis, the employment context makes the provision of consent very challenging as in this context it is difficult for an employee to give his/her *free* consent. Thus, another legal basis was recommended in D11.2, i.e. Article 7 (f) Directive 95/46/EC, pursuant to which a data processing operation could have a legal basis if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject…". However, an update to this recommendation is necessary, as in December 2015 the text of the General Data Protection Regulation was adopted. Pursuant to Article 6 (1) (f) therein, if the controller is a public authority and carries out the data processing in the performance of his tasks, he may not rely any more on this legal basis.[8] Thus, the eVACUATE end-users who are public authorities, may not be able to rely on this legal basis for the first responders app. Therefore, they should find another legal basis. For example, a controller may process personal data if this would be necessary for carrying

[8] Proposed General Data Protection Regulation, Council of the European Union Document number 15039/15.

out a task in the public interest.[9] However, it must be well motivated that the specific first responder app with its final features indeed represents a *necessity* when the end-users carry out their task in the public interest. As to the end-users, who are private authorities, then they could continue relying on Article 7 (f) Directive 95/46/EC (or Article 6 (1) (f) GDPR) if they strike the right balance between the needs of the controller and the risks to the employees.

In addition, the safeguards pointed out in D11.2 continue applying, namely informing the employees about the app before they download it, i.e. about its purpose and the processing of their data through it and recourse in cases of abuse of their data. The app should not be used to track the employees, especially when they carry the device also off-duty (unless they are required to carry the device all the time, e.g. if this is the case in the cruise ship scenario), or used as evidence for the actual working hours spent by them.

Last but not least, there are ethical concerns about such an app that should be considered. For example, such an app might result in higher expectations towards the first responders, e.g. more alerts being registered, faster responses expected, better results, etc. While such results could contribute to better alerts managements, more safety and security, it must be examined whether all situations can be adequately handled by the existing numbers of employees without undue burdens placed on them or whether more human resource will be needed.

2.2.3. App for missing people

An app for missing people on the cruise ship, i.e. those who have not mustered, has also been proposed.[10] The **purpose** of such an app has been explained to be helping the mustering personnel find the cruise passengers who have not mustered and who thus might be assumed to be in need of rescue. It is essential that the personal data processed through this app, like the other apps, is not processed for further, incompatible purposes such as tracking the staff member using the app. In this respect, the above discussion on the data protection considerations of the app for first responders applies here as well.

It should be noted that the information and personal details of passengers that would be displayed on the app should be only the one that is necessary in order to identify the persons who are missing. The personal data for this, as proposed by TELESTO, are the name, cabin number, family status and age of the passenger, as well as information whether he suffers from some disability. While identifiable information would certainly be necessary, it is recommended to process the information on a missing passenger's family status only if this information is proven to be necessary for the mustering and rescue tasks of the cruise personnel.

D11.2 examined the matter of connecting the app to the passenger database (which is part of the Hospitality Information System, in the case of the cruise ships it is the FIDELIO platform). It has been explained by TELESTO that the missing app will send

[9] Article 6 (1) (c) General Data Protection Regulation, Council of the European Union Document number 15039/15.
[10] As proposed by TELESTO in a PPT sent on 8.12.2015.

the names of the passengers who have mustered at the mustering station to the list of passengers (separate from the FIDELIO database). From the comparison of the names communicated from the app to this list one can see which passengers have not mustered. Then, an inquiry can be made to FIDELIO to ask about the details of the missing people, e.g. cabin number, picture. It is recommended that once the app knows who the missing people are, it retrieves from FIDELIO only the data on these missing people and does not randomly search the whole FIDELIO database. More precisely, this means that the hotel administration, which is in charge of FIDELIO, should communicate the necessary data on the missing people to the app after they receive the list of the passengers who have mustered (as it is currently done, although currently there is no such app). In addition, FIDELIO should send only the personal data on the missing passengers that is actually necessary for their rescue, excluding unnecessary data such as credit card numbers, etc. It is also recommended to check whether the ship administration rules will provide additional requirements and recommendations for the operation of such an app.

In conclusion, the different eVAMAPPs should be designed and operate in such a way as to ensure that the information needed for identification and location of individuals poses minimal risks to the privacy and data protection rights of individuals. In addition, the recommendations already provided in D11.2 continue to apply and should be considered.

2.3. SoNeMa Platform

2.3.1. Update on the concept and details of the platform

The social media that will be used by the eVACUATE solution for data mining purposes are **Twitter, Facebook, and Foursquare.** Their mining and the analytical operations performed on them will form part of the so-called SoNeMa Platform, as it has been presented by TELESTO.[11] For the eVACUATE validation demonstrations, SoNeMa will be tested only at the Anoeta Stadium in San Sebastian, Spain.[12]

The main objective of using SoNeMa in eVACUATE is to find and analyse the postings of individuals who have **public profiles**. The focus is on those who post **content**, such as status updates, which is in the public sphere and which is accessible to eVACUATE via public channels (e.g. Twitter, Facebook public statuses).

The **personal data** which SoNeMa will have access to and use are the profile name/alias, the profile picture, the content of the entries on the social media, and geolocation of the posts of interest to eVACUATE. In addition, *statistical data* such as demographic information, number of people checked-in at the premises of the end-users (via Foursquare API), the sentiment of the posts collectively, i.e. whether they are positive or negative, will be used. For that purpose, IBM's Alchemi engine will be used and thus the accuracy of the analysis is the responsibility of IBM.[13] Further data that will be processed is the fans/followers of the end-user facilities, and the KLOUT scores of the profiles that post the content of interest. The KLOUT score measures the influence of social media users across social media. The higher someone's KLOUT is, the more influential they are. The score is a number between 1 and 100 and this number is an accumulation of the influence of social media users across social networks.[14]

The search will be performed by using key-words related to situations that could relate to an emergency, such as flooding, fire, etc. However, it is understood that any status update/tweet that contains the name of the end-user will be selected and retained. *From a legal and ethical perspective it is recommended that the search terms should be narrowly defined so that the search engine of the SoNeMa platform targets content from the social networks that is relevant for the purposes of eVACUATE, i.e. emergency response.* This recommendation is especially valid for the real-life cases, when SoNeMa would be implemented in practice and proper search terms should be defined to improve the accuracy of the technology and limit the disproportionate collection of user-generated content, which contains personal data.

For the validation demonstrations it is contemplated that a special hash tag could be created, e.g. "#fp7evacuate" as mentioned in the scenario description from December 2015. The volunteers could be asked to write a message to be detected by SoNeMa in the course of the pilots, e.g. "FP7eVACUATE." If this is the case, then for the

[11] TELESTO presentation during a telco on 5/11/2015 and during the 2nd Review Meeting, 25 February, Brussels.
[12] Email from INDRA, 26.01.2016.
[13] Email from TELESTO, 10.11.2015.
[14] https://klout.com/corp/score.

validation demos this will be the targeted term, used as a search term and it is expected then that the search will be restricted to the postings by the volunteers.

As to the results from the datamining activity, it is understood that alerts raised by the SoNeMa will be only informative and will trigger no other automatic reaction, unless the personnel monitoring SoNeMa decides to react in a certain way following their interpretation of the SoNeMa content.

The current **purposes** of the SoNeMa Platform in relation to eVACUATE, as declared by TELESTO within WP7, are the following:

1. To find and evaluate conversations that take place in the social media and which are related to the pilots [especially for the pilots phase]. End goal is to offer alerts based on events of statistical importance.
2. Provide statistics on demographics, fans and followers, demographics, KLOUT score, sentiment analysis.

It is assumed that the purposes in real-life operational situations will be similar.

2.3.2. Ethical and legal analysis and recommendations

In the first place, as also explained in D11.2, except for the statistical data when it does not allow for identification of individuals, the above-mentioned data constitute **personal data** as they refer to information about identifiable individuals and their thoughts, location, profile picture, etc. This is the case even if the individuals are not always directly identifiable, i.e. they have only a user name or alias instead of their actual names, and even if the individuals who post on the social network *as such* are not of interest to eVACUATE. The reason is that through their social network identity individual people can be singled out from the rest and also eventually identified.

The fact that their postings are in the public sphere does not change the fact that the data processed are personal data. As explained in D11.2, data relating to identifiable individuals is still personal data even if it is publicly available as the data continues being related to identified or identifiable individuals. Therefore, the EU data protection legislation continues applying to SoNeMa both for the research/validation phase of the project and its operational phase. In addition, the controllers and/or processors for these activities are one or more of the eVACUATE partners, all of whom are established in the EU. The same would apply to operational situations when the controller or processor is established in the EU and/or (1) the processing of personal data of the data subjects happens in the context of offering goods and services to data subjects who are in the European Union, irrespective of whether the service is remunerated by payment by the data subjects, or (2) their behaviour is being monitored when their behaviour takes place in the European Union.[15] It needs still to be seen how the newly adopted text will be applied in the future, but it is certain from the text that it will apply to the data processing carried out by all emergency authorities established in the EU, as has been the rule also under Directive 95/46/EC.

[15] Article 3 of the adopted General Data Protection Regulation as adopted in December 2015, Council of the European Union Document number 15039/15.

With regards to the statistical data processed by SoNeMa, as long as the data is not personally identifiable and it is fully anonymized, it is not considered to be personal data as defined by the current EU data protection framework. However, if there are any risks that the statistical data can be re-personalized, e.g. by cross-linking it with other data which allows the re-identification of the persons, then the data should be treated as personal data.

2.3.2.1. Purpose specification and limitation, necessity and proportionality

One of the key data protection issues of SoNeMa is its compliance with the **purpose limitation principle**. Thus, there is a need for defining the **legitimate purposes** of SoNeMa more narrowly and more precisely *in relation to the purposes of eVACUATE*. Specifying the purpose is equally valid for the research and validation phase, as well as for the potential operational case in the future.

To that end one should bear in mind that the **purposes** of the project and of the eVACUATE solution are to define, update and maintain the Active Evacuation Route (AER) as a part of the emergency response in enclosed spaces. In the context of eVACUATE such situations should be clearly defined, e.g. those that relate to an emergency situation which are likely to trigger an evacuation, i.e. serious incidents. Thus, one should define the purpose of the SoNeMa datamining activity more narrowly to match the purposes of eVACUATE. An example of such a narrow definition would be limiting SoNeMa to identifying information on social networks that would inform the end-user of an incident that is taking or about to take place on their premises. However, it must be demonstrated through practical evidence that the existing technologies and/or practices used by the end-users are not sufficient in providing the information that SoNeMa seeks to provide, i.e. it must be proven that SoNeMa is a *necessary* response to the safety and security gaps experienced by the end-users. Thus, if security/safety events can be identified without mining the social networks, the proposed data mining should be avoided. In real-life situations the end-users should consider whether the SoNeMa should be active all the time and what information it seeks to collect in order to *avoid disproportionate* collection and analysis of user-generated content, on the basis of a careful necessity and proportionality test. For instance, if there are no matches at the stadium, e.g. ASRS, it would not be reasonable to operate the SoNeMa. During a match, it should be considered whether the events/incidents, which SoNeMa is supposed to detect, cannot be detected by the crew personnel who are present at the stands or alternatively through the security cameras. Similar reasoning applies to the other end-user sites, all of which normally have a high number of personnel present at the venue.

Once the necessity is demonstrated and the purposes are narrowly set in light of eVACUATE, then the *functionalities and operation* of SoNeMa should clearly correspond to these purposes and not go beyond them, i.e. they should be *proportionate* to these purposes (both for the pilots, the research and real-life operations). This concerns:

(1) **The targeted content**, i.e. searching only for posts that actually have significance for eVACUATE and refer to possible emergency situations. Thus, for example, the search terms of the social media should target only postings

that clearly refer to situations which could provoke an emergency, i.e. incidents such as floods, fights and fires, and not posts in general which refer to the end-users sites but do not refer to incidents and/or crowd management issues. This can be achieved by selecting carefully the search terms and restricting them to those that can discover emergency situations and not perform further big data analytics through this datamining operation.

(2) **The time range/span of the targeted statuses**. This means that since eVACUATE is focused on reacting to events which are happening in real time, the posts which actually matter are the ones from the present/current time. A fortiori, posts from previous days and years would simply not be useful for the eVACUATE case and would unnecessarily process personal data. In addition, the information provided by a search in the past might distract the decision-makers. Thus, such posts should be excluded by the search or alternatively automatically deleted by the technology. For the pilots, restricting the searches to information posted in the time span of the validation demonstrations would be a good example.

(3) **The analytics performed on the selected data**: geolocation, sentiment analysis, gender distribution and age, followers and fans overview, check-ins, influence analysis through KLOUT. While these business analytics could be of interest to the end-users for business purposes, it is questioned whether they are necessary for the purpose of eVACUATE, especially the number of fans and followers, demographics, the attitude of the people through sentiment analysis and the influence analysis of individual users over time. If the latter is used to estimate the reliability of postings, this can be achieved via human intelligence and spam accounts can be simply removed from the outset. With regards to the number of people checked-in, the question is whether they can be estimated by the video surveillance technology and humans on the ground. In addition, not everyone who is present on the premises will be actually checked-in. The same goes for geolocation, i.e. where the posting comes from - which country and city. It was explained by TELESTO that the purpose thereof is to find out whether the person posting about an end-user is actually closely located to the venue and thus whether his/her posting about a possible incident on the premises of the end-user is trustworthy. However, as TELESTO has explained, due to the Twitter API terms and conditions (T&C), SoNeMa will not search for the current location, as it was excluded from the license agreement of the use of the service.[16] Thus, the actual location of the person cannot be established with certainty and only the location of the person as indicated on his profile will be used. It is questioned in how far this geolocation information would be reliable.

Through the Foursquare API, SoNeMa will be able to obtain information on how many people have checked in at a certain location, which will be displayed on the demographic map made by SoNeMa,[17] showing a certain percentage of the individuals who are actually present at the venue.

[16] Email from TELESTO, 16.11.2015.
[17] Email from TELESTO, 10.11.2015.

(4) In relation to the **purpose limitation principle**, when personal information is collected as part of the emergency monitoring, one should take measures to prevent the re-use of the data for other incompatible purposes that might not fall within the sphere of competence of the end-users and their responsibilities regarding the safety of the crowds and their successful evacuation in emergency cases.

(5) Defining **a policy for deletion** of the unnecessary posts, as well as for the posts that are not relevant any more. For example, posts collected with regards to a certain football game would not be necessary once that football game is over. Thus, the timely deletion of the posts from the SoNeMa platform should be defined according to the needs of the particular end-user. In any case, storage periods longer than a couple of hours are discouraged and if the data is to be stored longer, such exception should be strongly motivated. Exceptionally, for the eVACUATE pilots longer periods would be acceptable to make evaluation and assessment of the performance of the technology during the pilots.

(6) As regards the **validation demos** during which the SoNeMa will be tested, it is understood from the scenarios that SoNeMa will be tested at AIA and at ASRS. Volunteers will be asked to tweet a message containing the word “evacuate”, using special hash tags, created for the exercise.[18] It is recommended to avoid confusion across the network that could ensue from tweets about incidents. One option could be to ask the volunteers during the demo to tweet terms which actually do not say “fire” or “incident” but rather a random term which will not lead to false alarms, e.g. “demo.”

2.3.2.2. Legal basis

The SoNeMa platform will mine user generated content from the above-mentioned social networks, including information that relates to an identified or identifiable person. As the Court of Justice of the European Union has established, activities such as datamining of content on the web constitute processing of personal data.[19] Therefore, the legal basis for this data processing needs to be established. Since SoNeMa offers the opportunity to search all possible content from the social networks, consent cannot be relied on as a legal basis as consent cannot be asked of everyone who is using social networks and could possibly be targeted by SoNeMa. This is especially the case for the operational, *real-life situations*.

It is understood that for the *validation demonstrations* there is a possibility to create a hash tag, with which the participating volunteers can post messages with key words, which will then be caught by SoNeMa’s search engine. If this is indeed the case and there is no risk that content not related to this predefined hash tag or to individuals who are not volunteers for the validation demonstrations will be caught by SoNeMa, then still consent can be relied upon. However, if despite the hash tag any content of social media users who are not associated with the demos and who have not given their

[18] eVACUATE scenarios from December 2015 as communicated via email by Pedro Garibi on 26.01.2016.

[19] Court of Justice of the European Union (CJEU), *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, 13 May 2014.

consent could be selected and analysed by SoNeMa, then consent should not be the only legal basis for the data mining activity. Therefore, another legal basis should be considered. Such other legal basis is necessary also for the research that TELESTO has already been performing in the past months by mining the social networks to train the features of SoNeMa.

For the **research activities** (performed by TELESTO) and the **validation demos**, one can consider other legal bases in Article 7 of Directive 95/46/EC, such as:

- Processing is *necessary* for compliance with a legal obligation to which the controller is subject. (Article 7 (c) Directive 95/46/EC)
- Processing is *necessary* in order to protect the vital interests of the data subject (Article (d) Directive 95/46/EC)
- Processing is *necessary* for the performance of a task carried out in the public interests or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. (Article 7 (e) Directive 95/46/EC)
- Processing is *necessary* for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1 (1). (Article 7 (f) Directive 95/46/EC)

All of these legal bases suggest that the data processing must constitute a "necessity." To pass the necessity requirement, a certain measure, such as SoNeMa has to be more that simply "useful," "reasonable," "ordinary," "admissible," "desirable."[20] Therefore, a strong motivation and proof as to the actual necessity should be demonstrated. Since in the research and validation cases one can argue that the mere research and validation do not relate to an actual necessity to protect someone's vital interests, or to perform one's legal obligation or a task in the public interest, then the only remaining option is Article 7 (f). It requires a careful balancing of the interests of the controller, i.e. TELESTO and possibly other controllers from the eVACUATE consortium during the different validation demos, and of the data subjects, i.e. social network users in general in view of the risks to their privacy. The following paragraphs explain how relying on this legal basis for the research and validation activities for SoNeMa fulfils the requirements of Article 7 (f). As Article 29 Working Party has explained, the following criteria have to be considered when applying Article 7 (f):

- The data processing has to be lawful (in accordance with the applicable EU and national laws),
- The legitimate interest of the controller has to be clearly articulated and specific,

[20] Quote ECtHR in the case of *Handyside*. The term "necessary" here is defined by the ECtHR in the context of Article 8 ECHR. However, as the CJEU ruled in the *Österreichischer Rundfunk* case, the provisions of Directive 95/46/EC must be interpreted in light of fundamental rights such as the right to privacy. Thus, for the purposes of applying the Directive, including Article 7 thereof, it must be first examined whether the data processing measure provides for interference with private life and whether this interference is justified in view of Article 8 ECHR, including whether it is "necessary in a democratic society."

- The data processing should present a real and present interest.[21]

First of all, TELESTO as the controller for the research part and possibly one of the controllers for the validation demonstrations has a **legitimate** *research* **interest** in developing new technologies which can be used to detect incidents, testing their features and validating them against real-life scenarios. Possibly these new technologies, such as SoNeMa, after its feasibility and usefulness has been proven in the particular real-life applications it can be applied in, can bring about improvements to the work of the emergency personnel. For the usefulness and necessity of such technological improvements to be examined, the technology needs to be developed and validated against the real data coming from social networks. As the Article 29 Working Party has also indicated, research activities can be considered to constitute a legitimate interest, although Article 7 (f) does not give a blanket permission to re-use and further process publicly available personal data, such as the personal data available on social media.[22] Thus, this legitimate *research and validation* interest would be acceptable for the duration of the eVACUATE project. It also appears that these research interests are relatively specific and clear enough for the research case. As to the first point on lawfulness, it is examined in the paragraphs below.

As the Article 29 Working Party has highlighted, the legitimate interest of the controller has to be balanced against the **interests and fundamental rights and freedoms of the data subjects**. Thus, appropriate measures to mitigate the privacy and data protection risks should be taken.[23]

It is noted here that SoNeMa targets only publicly available content, excluding any content not meant to be public such as private messages or profiles and content which is accessible only to a limited number of friends, for example. Therefore, the privacy and data protection risks are diminished. In addition, to prevent further risks for the data subjects, TELESTO is advised to comply with the purpose limitation principle and not use the SoNeMa data for further purposes beyond research in the framework of eVACUATE. As has been highlighted many times, data security must always be complied with to avoid illegal access to the personal data. Furthermore, TELESTO is advised to collect from the social networks only the minimum necessary data and to delete the rest, as explained above. Thus, also the data minimization principle will be complied with. In addition, the SoNeMa platform does not intend to profile individual social media users and to process any sensitive information concerning them. While it has an interest in knowing their KLOUT score to measure their influence and determine whether the status updates are spam or not, it is advised that if this feature is not necessary, it should be dispensed with and human intelligence should delete the spam accounts from SoNeMa. However, even if it is kept, it should not lead to profiling of the

[21] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC, WP 217, 9 April 2014; Kuczerawy A., et al, REVEAL Deliverable 1.2b: "Legal/regulatory requirements analysis: Processing Personal Data from Social Media and Social Media API Terms and Conditions," 30.10.2015.

[22] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC, WP 217, 9 April 2014

[23] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC, WP 217, 9 April 2014

individual users and taking decisions which can affect them. The platform should not produce legal effects on the data subjects in general.[24] As TELESTO has explained, KLOUT will only serve as a filter, to shortlist tweets that really matter, against spam accounts. Thus, to minimize the risks, it is advisable that indeed SoNeMa is used only to obtain information about a possible incident and not to monitor users' behaviour and use them to surveil these people and possibly send the police to them, e.g. during a football game. In reality such an event occurred in Antwerp, Belgium, in the fall of 2015, when *a student was arrested* and a building was evacuated following an ironic, but innocent tweet exchange between two students in the framework of a networking event.[25] Amongst the problematic issues in this case is that the personnel immediately called the police who arrested people without really looking at what was written in the tweets, i.e. human intelligence was not involved, and a tweet exchange caused an immediate police action which resulted in unjustified arrests. This points to the problems of overreliance on user generated content. On the other hand, it is questionable whether serious crimes are planned publicly over social networks.

It is acknowledged that it is difficult to inform the data subjects of the research carried out with their postings, and thus to be transparent. However, as per Article 11 (2) Directive 95/46/EC, the controller is exempt from the obligation to inform the data subjects of the processing of their data if the provision of this information would require disproportionate efforts.[26] Only the volunteers taking part in the eVACUATE demonstrations events can be effectively informed. Nevertheless, TELESTO is advised, if contacted by a social networks user who makes an inquiry about a potential processing of his data by TELESTO in the framework of the eVACUATE SoNeMa and requests the deletion of his data, to fulfil the request of the data subject. While the legal compliance of the validation demonstrations will be elaborated on more in the following months, it can be contemplated informing the public through the eVACUATE or end-user websites that social network data-mining concerning posts mentioning the end-user site will be performed for research purposes and allow individuals to make an inquiry about the processing of their posts and other data.

Last but not least, TELESTO has committed to comply with the API requirements of the respective social networks as listed in their respective Terms and Conditions. It is expected that the requirements stemming from the EU level legislation on data protection will be complied with, guidance of which is provided in the present deliverable.

For **operational cases** after the General Data Protection Regulation (GDPR) enters into force, it will not be possible to rely on Article 7 (f) Directive 95/46/EC (or rather Article 6 (1) (f) GDPR) if the controller is a public authority (see discussion above in the section on the smartphone app). While the other legal bases enumerated in the paragraph above are a possible candidate, the strict necessity of the SoNeMa platform

[24] Kuczerawy A., et al, REVEAL Deliverable 1.2b: "Legal/regulatory requirements analysis: Processing Personal Data from Social Media and Social Media API Terms and Conditions," 30.10.2015, p. 11-12.
[25] http://deredactie.be/cm/vrtnieuws.english/Antwerp/1.2457373
[26] Kuczerawy A., et al, REVEAL Deliverable 1.2b: "Legal/regulatory requirements analysis: Processing Personal Data from Social Media and Social Media API Terms and Conditions," 30.10.2015.

as such and its individual features in particular for the performance of someone's duties or tasks in the public interest will have to be proven, i.e. that without SoNeMa information about possible incidents cannot be obtained. This discussion on the necessity of the technology in the context of eVACUATE should also be taken into account when performing the balancing test of Article 6 (1) (f) GDPR if its usage legal and an end-user intends to rely on it.

2.3.2.3. Additional legal requirements

In addition, since SoNeMa will make use of the APIs of Twitter and Foursquare (which will be used to check the aggregate number of check-ins at a certain location), their respective Terms and Conditions (T&C) for usage should be complied with. Since these T&C are subject to change, they should be constantly monitored. A copy of these T&Cs as of 22 January 2016 is provided in Annex I.

According to the **Twitter API**, the requirements for its legal usage are plenty and TELESTO is advised to comply with all of them. While the full content of the Twitter API can be found in Annex I, certain points in the Annex have been highlighted in yellow, as they are especially relevant for eVACUATE. For example, the guidelines on respecting the user's control and privacy are especially topics. It is also observed that the API T&C forbid any usage of location and geographic data on a standalone basis, unless the data is processed as a part of a tweet.[27] Another example is the prohibition to use material which is private. It is noted that eVACUATE will not access content which is not public, as promised by TELESTO.

If eVACUATE would allow users to publish content on it, there are certain requirements, which are marked as text in red in Annex I. For example, in such cases the service provider should clearly inform those who will post of how their information will be used and which information will be used, including whether geo tags will be added, and obtain permission to use the content.

According to the **Foursquare API**, which will be used to check how many people have checked in at a certain place, the T&C of Foursquare advise the following: "Licensee shall not use the Foursquare Materials in connection with or to promote any products, services, or materials that constitute, promote or are used primarily for the purpose of dealing in: … emergency or life-saving purposes." (see Annex I). Thus, the location information obtained via Foursquare should not be used as input to the strategic decisions related to the safety and evacuation procedures. For real-time route guidance, licensees should have an end-user agreement, where it is indicated that the usage of Foursquare for these purposes is at the risk of the end-users.

2.3.2.4. Ethical considerations

The collected data and the analytical results displayed to the decision-makers should be considered not solely in light of the data protection and privacy principles. This means that even when SoNeMa does not process personally identifiable data but only statistical data, there could nevertheless be negative impact on the eVACUATE end-

[27] Last point under Clause 2 of the Twitter API T&C.

users and the social media users. In that respect there a number of ethical and practical issues to consider, namely:

1. Unnecessary personal data processing contravenes not only the data minimization, purpose limitation, necessity and proportionality principles. It would not be ethical to access user-generated content for *purposes* either strictly not necessary for eVACUATE or to access *information* which as such is not necessary for eVACUATE, e.g. of past events to which the end-users cannot react anyway, but would just obtain additional information about individuals and events. This is valid both in the research/validation and operational cases.
2. Another ethical issue is statistical data. While statistical data in itself does not display information on identified individuals, one still needs to consider the technical risks of de-anonymizing the data sets and take the necessary steps to avoid such risks.
   In addition, one should note that statistical information is produced by collecting and further processing personal information. This means that for someone to obtain anonymized datasets, one still accesses, collects and analyses the information on the individual Twitter and Facebook users (even if the operation is not performed by eVACUATE but the statistical data is directly received by eVACUATE from Twitter and Facebook APIs). And even if the risks for individual social media users are minimized, the fact remains that the knowledge produced provides a rich set of information on crowds and their patterns, behaviour and/or attitudes, which enhances the opportunities for surveillance of groups of people, extracting knowledge on attitudes and behavioural characteristics, and also possibly on specific individuals (who might be identified through the collection and cross-linking of statistical data).
3. From an ethical and practical aspect, displaying more information than strictly necessary in the context of eVACUATE could be distracting for the end-users. One should not forget that the end-users (those in eVACUATE and also other prospective end-users who are not members of the eVACUATE consortium) are safety and security personnel, who normally dispose only of short time to react to a certain emergency situation. Thus, one should focus on showing to them only information which is necessary for their tasks. Thus, it must be seen whether all the business intelligence analysis performed by SoNeMa would be essential information for the decision-makers. While there could be an opportunity for a modular architecture and the end-user can decide to close or minimize certain fields, e.g. those on the friends and followers, this might not be an optimal solution in emergency cases, where unnecessary information could distract and confuse the emergency personnel and unnecessary time might be spent on closing screens. The question is whether security and safety personnel need to know how many people have checked in at a specific venue, how many friends and followers the venue has, what the age and gender distribution of those checked-in is (who might also not be representative of the actual distribution), the sentiment analysis, etc. It is not only that such information could distract the end-users, but also that user-generated content cannot be fully trusted and thus its reliability is questioned. Thus, the usefulness and practicality

of the features of the SoNeMa should be carefully assessed by the personnel who will actually interact with the eVACUATE platform.

In conclusion, information from social networks could be useful in certain emergency situations. To minimize the privacy risks on individuals and increase the usefulness and accuracy of the data provided to first responders, it is important to focus on the purposes of the SoNeMa, the way information is targeted, as well as the analysis performed on it. Most importantly, the necessity of its features should be motivated. In addition, the proper legal basis for its operation, especially in operational situations should be defined.

2.4. (Crowd) behaviour detection

2.4.1. Introduction

Following up on the discussion from D11.2, this chapter will analyse the additional legal and ethical issues raised in eVACUATE with regards to the crowd behaviour detection technology performed by video monitoring and analytical technologies, as developed in eVACUATE, especially in WP3. The analysis will take into account the technology elements which were reported in eVACUATE deliverables D 3.2 and D 3.4, as well as the presentations given at project meetings, i.e. in Manchester/UK (July 2015) and St. Nazaire/France (October 2015). Next to the privacy, data protection and ethical issues which such monitoring and analytical technologies raise in principle, the discussion will focus in more detail on the person detection and finding features of people in crowds and looking for "unique persons in crowds."[28]

Before elaborating on the discussion in D11.2, the following paragraph will make a recap of the analysis and recommendations concerning the crowd behaviour detection technology as discussed in D11.2. These were namely:

1. *Legality* of using behaviour detection algorithms. This relates to the question of whether a proper *legal basis* exists for carrying out crowd behaviour monitoring technologies in European law and also in the laws applicable to some of the eVACUATE end-users (when such information was available), what adequate *safeguards* for individuals should be put in place to avoid arbitrariness, and whether the measure is *necessary and proportionate* to the purpose pursued, i.e. studying crowd behaviour as a part of designing the Active Evacuation Route (AER).
2. Intimately related to this is the requirement for a *narrowly specified purpose* in order to avoid illegal and unethical data re-use/abuse and to define properly whether each feature of the technology is necessary and proportionate.
3. The technical possibility to *single out, distinguish and recognize specific individuals* who are members of the crowd. This could happen if specific people have features that single them out, e.g. much taller people who stand out and whose faces can be recognized, or by detecting specific behaviour of selected individuals. This challenges the anonymity of people in the crowds and raises

[28] AS presented during the St Nazaire meeting/France (October 2015).

further ethical, privacy and data protection concerns. It also poses risks, as it is a profiling technique, e.g. of obtaining more knowledge about individuals which might be excessive for the purposes of evacuation.

4. *Accuracy and reliability* of the technology and its results, e.g. false events might be detected and trigger alarms or behaviours could be wrongly classified as being "usual" or "unusual".
5. *Profiling* and especially the *accountability* for the produced results, i.e. attribution of responsibility for the conclusions of the technology and automating human knowledge.
6. Ensuring an adequate level of *data security*.
7. Keeping this automated behaviour detection technology *dormant* when a given situation does not necessitate the operation of this technology. Each end-user should assess whether the situation necessitates the operation of the algorithms and the automated behaviour detection. More guidance could be found also in the opinions of the data protection authorities in the respective countries. This is without prejudice to the normal operation of the CCTV cameras at end-user premises as currently allowed and carried out in accordance with the applicable law to which the eVACUATE end-users are subject. The issue is the *necessity* of *always* having the *behaviour detection algorithm* switched *on*. Even if the (crowd) behaviour detection technology does not aim at or result in the monitoring and tracking of *individuals,* it still could result in extracting knowledge about crowds that could be negatively used by those having access to the tool, which thus raises ethical issues.

2.4.2. Further legal and ethical analysis

Some of the conclusions from D11.2 summarized above contain recommendations, which continue to apply until they are fully addressed, e.g. ensuring data security when the whole solution is put together and installed at the end-user premises both during the pilot demonstrations and in operational situations.

It is acknowledged that in WP3 further work has been done with regards to the **accuracy** of the technology, as reported during the meeting in St. Nazaire. However, accuracy challenges still persist. As indicated by ITINNOV during the St. Nazaire meeting (October 2015), the analysis of the recordings at AIA indicated that, e.g. reflections were counted as people. Another accuracy issue is the interpretation given by the algorithms. Since in literature abnormality is defined as a statistical or other deviation from the current situation,[29] the possibility for wrong interpretations even if the algorithm in itself functions properly, is *per se* embedded into the technology and cannot be eliminated. It is acknowledged that ITINNOV has performed work on interpreting the context to enhance the accuracy of the analysis of the algorithms. In this way, the technology is supposed to work more precisely. However, this does not eliminate the problem that still the classification of behaviours remains a statistical probability which cannot always be accurate. In addition, even such technologies

[29] eVACUATE Deliverable D 3.4 "Multi Scale Behavior Recognition_v2," p.14.

cannot be 100% neutral as human beings determine the idea of normality and abnormality, which are then translated in algorithms.

In the further analysis of the technology in the present deliverable the focus will be a more detailed analysis of the legal and ethical risks of the technology with regards to the automated analysis of *crowd behaviour* and possibly the behaviour of *specific individuals* or *small groups* thereof. The purpose is to study the impact of the technology on the fundamental rights of individuals, based on the assumption that the purpose of the technology **is not to identify/recognize** individuals. The eVACUATE technology is interested in human activity recognition and behavioural understanding of the crowd as a whole, as well as certain individuals in it, e.g. active participants in the crowd that could stand out.[30]

Behavioural and psychological characteristics are classified as soft biometric data, which make features of the human body machine-readable and subject to further analysis and use. Examples of such biometric data are gait analysis and way of moving and walking.[31] In the case of eVACUATE, the biometrics characteristics of individuals or groups of individuals would be used not for purposes of identification and verification, but for purposes of categorization, i.e. to assign an individual to a specific group of predefined characteristics (usual or unusual behaviour) and possibly take actions on the basis of this categorization, e.g. subject someone to closer monitoring.[32] While eVACUATE is interested in identifying whether something unusual is happening, the identification of unusual events could lead to flagging specific parts of the crowd or even individuals who are classified as seeds. Possible actions that could be taken as a result of this flagging are monitoring more intensely a specific area and/or people, determining the course of action during evacuation, sending the police to tribunes which are deemed to behave unusually during a football game, etc.

The cameras that are/will be used in eVACUATE are optical, thermal and hyperspectral (infrared). Only the optical ones allow/enable direct identification of individuals. However, the thermal and hyperspectral streams, when combined with optical ones, can lead not only to the identification of individuals. This combination can reveal further information about crowds and individuals, e.g. temperature, which adds to the knowledge that can be obtained on (specific) individuals or groups thereof. The hyperspectral and thermal cameras can also enhance the detection possibilities of the optical cameras.[33] For example, higher temperature could signal nervousness. In the December 2015 version of the STX scenario, there is a proposal to use thermal and hyper-spectral cameras to detect the presence of people, who are not evacuating after the evacuation has started, close to an elevator. Thus, crew personnel could be sent to them to evacuate them. While such a use of the thermal and hyper – spectral cameras bears no or minimum privacy risks, it should be ensured that the technology

[30] eVACUATE Deliverable D 3.4 "Multi Scale Behavior Recognition_v2," p. 80 – 82.

[31] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, 27 April 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf, p. 4.

[32] Ibid, p. 6

[33] See Chapter 4.3 "Detection methods based on hyperspectral data" of deliverable D3.4 "Multi Scale Behavior Recognition_v2."

can recognize that these are passengers who are not evacuating and not crew personnel who is there to actually help people. This is to avoid false alarms.

While recognizing and knowing the identity of individuals is not aimed at by the eVACUATE technology, one should acknowledge and address two risks: (1) the risk of (unintentional) identifiability and recognisability of individuals, and (2) further privacy risks even if one assumes that the crowd remains anonymous and the people in it are anonymous, e.g. when one looks at the knowledge that can be obtained from behaviour recognition, which is classified as soft biometrics by Article 29 Working Party.

With regards to (1), as has been explained by WP3, the technology does not seek to identify and recognize individual people, or analyse their faces, facial expression, etc. This has also been the assumption of the legal analysis so far. Nevertheless, as argued in D11.2, technically speaking the risk cannot be eliminated that individuals can be recognized, e.g. if an individual comes closer to one of the cameras. In addition to this, further knowledge about individuals can be obtained with the help of the behaviour analysis features. For example, as indicated in D3.2, the project has an interest in being able to identify seeds, e.g. individuals who become leaders in the course of an evacuation, through the behaviour detection technology.[34] Their behaviours would stand out from the rest. This would allow the individual behaviours to be studied, including their effect on others,[35] and tracked,[36] no matter whether the person is identifiable or not. Thus, the risk becomes twofold: on one hand certain individuals can be recognized, on the other hand their behaviour (and/or the behaviours of others) and even their psychological state could be revealed and individuals singled out on the basis of their behaviour, even if their identity is not known. For example, if a person is not moving, but lingering in a certain area for a longer period of time, the algorithm might flag the person as “unusual.” As a result, he might be assumed to be somehow suspicious.

With regards to (2), the Working Party 29 has argued in its opinion on anonymisation and working with anonymized data that even when one processes properly anonymized data, i.e. works with data of unidentified individuals, one should still study the impact of such processing on individuals under certain circumstances, especially when it comes to profiling. In the context of eVACUATE a similar reasoning can be applied to profiling of the behaviour of crowds, which, as explained above, could result in singling out individuals, even without being interested in their identity, but only in their behaviour. For example, if the crowd as a whole is considered to be relatively calm and moving slowly, any individual who starts moving faster would be immediately detected and possibly flagged and monitored more closely. The Article 29 Working Party opinion reminds that the even when the data protection law as such does not apply to a certain data processing, the fundamental right to privacy continues to apply, protecting people’s private sphere from unnecessary and disproportionate interferences. Thus, loss of privacy may result even from anonymous data, e.g.

[34] eVACUATE Deliverable D 3.2 “Crowd psychology and typology classification_v2,” p. 26.
[35] *Ibid.*
[36] eVACUATE Deliverable D 3.4 “Multi Scale Behavior Recognition_v2,” p.34.

releasing anonymous datasets to third parties as explained by the Working Party. This anonymous set of data could be used to take decisions that produce effects, even only indirectly, on certain individuals.[37] In the context of eVACUATE the possible risks of the behaviour detection and monitoring technology with regards to the individuals' private sphere concern their being singled out from the rest and monitored. In addition, negative assumptions that can be made about them on the basis of their different behaviour, as explained at the beginning of the paragraph. Last but not least, when the models of what is "usual" or "unusual" are being constructed, the criteria of usualness are defined on the basis of the behaviour of certain people (e.g. a study group), even when they are anonymous, and then this common behaviour is being applied to other crowds and individuals, whose behaviour is assessed based on the behaviour of the previous group.

As the Article 29 Working Party indicates, soft biometrics or traits (e.g. gait and behaviour recognition) are not suitable to clearly distinguish or identify an individual. Nevertheless, they could enhance the performance of other identification technologies.[38] Therefore, a related risk, in the context of eVACUATE, is the risk of combining the behaviour detection algorithm with identifiable data, e.g. with optical video recordings and/or with other data available to the end users, e.g. the cruise ship lists of passengers and their names and contact details from the FIDELIO database. Thus, a specific person might become more easily identified on the basis of his behaviour. The data interlinkage increases the identifiability opportunities of the CCTV. Thus, the additional analytics provided by the behaviour detection and analysis algorithm can lead to the extraction of more knowledge on groups or specific individuals.

The real negative impact on the crowds or individual members of it is (a) the analysis of their behaviour and predicting their future actions and (b) the possible misuse of such analysis. This could happen if such a technology is used to detect, e.g. leaders during political gatherings, using crowd monitoring techniques for political and repressive purposes, e.g. during protests and other political initiatives, which might have a chilling effect on such crowd gatherings.[39] While such a risk has not been identified in the framework of eVACUATE as the purposes of the project are not to monitor politically motivated gatherings, it is reminded here that the software, such as the one developed in eVACUATE, might be used by different end users (different from the eVACUATE end-users) in operational context not related to eVACUATE for such political purposes as given in the example in this paragraph and such a usage could have a negative effect on the monitored individuals.

Last but not least, an important legal matter to address is the *transparency* of the technology and the logic behind its operation. It must be highlighted that for the functioning of this technology – the behaviour detection algorithm - no collaboration of the individuals is needed. Their data is being collected on the move, from a distance, and the logic of the profiling algorithms is not known to them, i.e. what behaviour will

[37] Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques, 10 April 2014, p. 11.
[38] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, 27 April 2012, p. 16.
[39] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, 27 April 2012, p. 17

be deemed as "unusual."[40] Currently, many of the CCTV systems have an information notice, informing the ordinary people that cameras are in operation, sometimes indicating also the law on which basis they operate. While individuals, when they are aware of the existence of cameras, assume that they are being watched, they can hardly assume about the level of sophistication of the technology, i.e. that it can automatically classify, analyse and predict their behaviours. Thus, the new features of the technologies should also be reflected in the information notices.

2.4.3. Conclusion

This chapter examined the issues related to the new behaviour detection technology not only from a data protection point of view. It also studied the broader privacy, as well as ethical implications with regards to the risks the technology poses on individuals. It repeats the recommendations provided in D11.2 and provides an additional one concerning the transparency of the technology towards the common people. With regards to the question whether this technology should be on at all times (without prejudice to the normal functioning of the CCTV cameras as allowed presently by law), it is noted that while for the validation demonstrations this could be acceptable as the functioning of the technology must be demonstrated in a short period of time, the same argument might not apply in operational situations. This means that when future end-users use this behaviour monitoring software, assuming a proper legal basis for its operation can be found for their premises, it should be considered whether this algorithm should be operational all the time as during non-busy hours or non-controversial matches the algorithms might not fulfil the *necessity* criterion.

[40] *Ibid*

3. Conclusion

The present deliverable examined in more detail specific elements of the eVACUATE solution, i.e. the chipless RFID technology, the eVAMAPPs, the SoNeMa and the CCTV behavioural monitoring and profiling. The purpose of the deliverable was to provide recommendations to these technologies in view of their data protection, privacy and ethical compliance. The analysis and recommendations seek not only to guide the partners in the final design of the technical solution and the potential exploitation of the technologies, but also to advance the academic debate regarding the usage of Information and Communication Technologies (ICTs) in emergency situations to manage crowds and people with regards to the ethical and legal issues surrounding the usage of these ICTs.

While the *data security* of the eVACUATE solution and its components, as well as *transparency*, *accountability, purpose limitation, accuracy, data minimization and regular personal data deletion* feature as common concerns and recommendations for each component, there have been specific legal and ethical issues with regards to the individual technologies:

- **Chipless RFID application**: the additional remarks concern the voluntariness of the application and the accuracy of the data and its practicality in the particular scenarios.
- **eVAMAPP**: this technology could bring advantages to both ordinary people and first responders. However, the discussed issues related to tracking and identifiability of the individuals should be resolved.
- **SoNeMa**: the legal basis has been considered as well as the necessity and proportionality of individual features of the SoNeMa.
- **Behaviour detection:** the analysis focused especially on the risks of identifiability, singling out and analysing the behaviours of individuals, as well as the negative consequences this could have on them.

It is recommended that in operational situations the end-users consider carefully whether the individual technology components as well as the whole eVACUATE solution should be operational at all times, on the basis of a detailed necessity and proportionality assessment.

If the data are used for **training purposes** even in operational situations, proper **anonymization** measures should be taken.

These concerns should be addressed not only by the technology producers, but also in the internal policies of the end-users who operate them to make sure that the functioning of the ICTs is privacy and data protection compliant.

4. Bibliography

Legislation:

Charter of Fundamental Rights of the European Union, OJ C 2008/C 364/01

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 the free movement of such data, O.J. L 281, 23.11.1995

Proposed General Data Protection Regulation, Council of the European Union Document number 15039/15

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and electronic communications)

Case-law:

Court of Justice of the European Union, SABAM, C – 70/10, 24 November 2011

Court of Justice of the European Union (CJEU), *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, 13 May 2014

ECtHR, *Handyside v United Kingdom*, Application Nr. 5493/72, 7 December 1976

Court of Justice of the European Union (CJEU), *Österreichischer Rundfunk*, Case C-465/00, 138/01, 139/01, 20 May 2003

Opinions, academic sources, articles:

Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC, WP 217, 9 April 2014

Kuczerawy A., et al, REVEAL Deliverable 1.2b: "Legal/regulatory requirements analysis: Processing Personal Data from Social Media and Social Media API Terms and Conditions," 30.10.2015

FlandersNews.be, "Building evacuated after ironic tweet," 1.10.2015, http://deredactie.be/cm/vrtnieuws.english/Antwerp/1.2457373

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007

Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, 27 April 2012

Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques, WP216, 10 April 2014

Time.lex, "Study of case law on the circumstances in which IP addresses are considered personal data, D3. Final Report," SMART 2010/12. 2 May 2011

Annex I: Terms and Conditions (T&C)

Twitter: [41]

I. Guiding Principles

1. A Few Key Points

a. Keep any API keys or other access credentials private and use only as permitted.
b. Respect our requirements on how to display and interact with users' content.
c. If your application will need more than 1 million user tokens, you must contact us about your Twitter API access, as you may be subject to additional terms.
d. Twitter may monitor your use of the Twitter API to improve the Twitter Service, examine commercial use and ensure your compliance with this Policy.
e. Remember, Twitter may suspend or revoke access to the Twitter API if we believe you are in violation of this Policy. Do not apply for or register additional API tokens if Twitter has suspended your account. Instead, contact us.

2. Maintain the Integrity of Twitter's Products

a. Follow the Display Requirements and Twitter Rules. If your Service facilitates or induces users to violate the Twitter Rules, you must figure out how to prevent the abuse or Twitter may suspend or terminate your access to the Twitter API. We've provided guidance in our Abuse Prevention and Security help page.
b. If your Service submits content to Twitter that includes a Twitter username, submit the correct Twitter username ("@username").
c. Promptly respond to Content changes reported through the Twitter API, such as deletions or the public/protected status of Tweets.
d. Do not modify, translate or delete a portion of the Content.
e. Maintain the features and functionality of Content and Twitter API. Do not interfere with, intercept, disrupt, filter, or disable any features of Twitter or the Twitter API, including the Content of embedded Tweets and embedded timelines.
f. Only surface Twitter activity as it surfaced on Twitter. For example, your Service should execute the unlike and delete actions by removing all relevant Content, not by publicly displaying to other users that the Tweet is no longer liked or has been deleted.
g. Do not exceed or circumvent limitations on access, calls, sharing, privacy settings, or use permitted in this Policy, or as otherwise set forth on the Developer Site, or communicated to you by Twitter.
h. Do not remove or alter any proprietary notices or marks on Content or the Twitter API.
i. Do not (and do not allow others to) aggregate, cache, or store location data and other geographic information contained in the Content, except as part of a Tweet.

[41] https://dev.twitter.com/overview/terms/policy, accessed 22 January 2016.

Any use of location data or geographic information on a standalone basis is prohibited.

3. Respect Users' Control and Privacy

a. Get the user's express consent before you do any of the following:

i. Take any actions on a user's behalf, including posting Content, following/unfollowing other users, modifying profile information, or adding hash tags or other data to the user's Tweets. A user authenticating through your Service does not constitute user consent.

ii. Republish Content accessed by means other than via the Twitter API or Twitter other tools.

iii. Use a user's Content to promote a commercial product or service, either on a commercial durable good or as part of an advertisement.

iv. Store non-public Content such as direct messages or other private or confidential information.

v. Share or publish protected Content, private or confidential information.

b. Take all reasonable efforts to do the following, provided that when requested by Twitter, you must promptly take such actions:

i. Delete Content that Twitter reports as deleted or expired;

ii. Change treatment of Content that Twitter reports is subject to changed sharing options (e.g., become protected); and

iii. Modify Content that Twitter reports has been modified.

c. If your Service allows users to post Content to Twitter, then, before publishing, show the user exactly what will be published, including whether any geo tags will be added to the Content.

d. If your Service allows users to post Content to your Service and Twitter, then, before publishing to the Service:

i. Explain how you will use the Content;

ii. Obtain proper permission to use the Content; and

iii. Continue to use such Content in accordance with this Policy in connection with the Content.

e. Display your Service's privacy policy to users before download, installation or sign up of your application. Your privacy policy must be consistent with all applicable laws, and be no less protective of end users than Twitter's Privacy Policy located at http://twitter.com/privacy. You must comply with your privacy policy, which must clearly

disclose the information you collect from users and how you use and share that information, including with Twitter.

f. If your Service uses cookies, disclose in your privacy policy: (in case this applies to eVACUATE)

i. Whether third parties collect user information on your Service and across other websites or online services;

ii. Information about user options for cookie management and whether you honour the Do Not Track setting in supporting web browsers.

g. If your Service adds location information to users' Tweets:

i. Disclose when you add location information, whether as a geo tag or annotations data, and whether you add a place or specific coordinates.

ii. Comply with Geo Developers Guidelines if your application allows users to Tweet with their location.

h. Do not store Twitter passwords.

4. Clearly Identify Your Service

a. Make sure users understand your identity and the source and purpose of your Service. For example:

i. Don't use a name or logo that falsely implies you or your company is related to another business or person.

ii. Don't use a shortened URL for your Service that attempts to mask the destination site

iii. Don't use a URL for your Service that directs users to

1. a site that is unrelated to your Service
2. a site that encourages users to violate the Twitter Rules
3. a spam or malware site.

b. Do not replicate, frame, or mirror the Twitter website or its design.

5. Keep Twitter Spam Free

a. Follow the Abuse and Spam rules here.
b. Comply with the automation rules if your Service performs automatic actions.
c. Do not do any of the following:

i. Mass-register applications.

ii. Create tokens/applications to sell names, prevent others from using names, or other commercial use.

iii. Use third-party content feeds to update and maintain accounts under those third parties' names.

iv. Name squat by submitting multiple applications with the same function under different names.

v. Publish links to malicious content.

vi. Publish pornographic or obscene images to user profile images and background images.

6. Be a Good Partner to Twitter

a. Follow the guidelines for using Tweets in broadcast if you display Tweets offline.
b. If you provide Content to third parties, including downloadable datasets of Content or an API that returns Content, you will only distribute or allow download of Tweet IDs and/or User IDs.

i. You may, however, provide export via non-automated means (e.g., download of spread sheets or PDF files, or use of a "save as" button) of up to 50,000 public Tweets and/or User Objects per user of your Service, per day.

ii. Any Content provided to third parties via non-automated file download remains subject to this Policy.

c. Use and display Twitter Marks solely to identify Twitter as the source of Content.
d. Comply with Twitter Brand Assets and Guidelines.
e. Do not do any of the following:

i. Use a single application API key for multiple use cases or multiple application API keys for the same use case.

ii. Charge a premium above your Service's standard data and usage rates for access to Content via SMS or USSD.

iii. Sell or receive monetary or virtual compensation for Tweet actions or the placement of Tweet actions on your Service, such as, but not limited to follow, retweet, like, and reply.

iv. Do not use, access or analyse the Twitter API to monitor or measure the availability, performance, functionality, usage statistics or results of Twitter's products and services or for any other benchmarking or competitive purposes, including without limitation, monitoring or measuring:

1. the responsiveness of Twitter websites, web pages or other online services; or
2. aggregate Twitter user metrics such as total number of active users, accounts, user engagements or account engagements.

v. Use Twitter Content, by itself or bundled with third party data, to target users with advertising outside of the Twitter platform, including without limitation on other

advertising networks, via data brokers, or through any other advertising or monetization services.

vi. Use Twitter Marks, or Twitter Certified Products Program badges, or similar marks or names in a manner that creates a false sense of endorsement, sponsorship, or association with Twitter.

vii. Use the Twitter Verified Account badge, Verified Account status, or any other enhanced user categorization on Twitter Content other than that reported to you by Twitter through the API.

7. Avoid Replicating the Core Twitter Experience

a. Twitter discourages online services from replicating Twitter's core user experience or features.
b. The following rules apply solely to Services or applications that attempt to replicate Twitter's core user experience:

i. You must obtain our permission to have more than 100,000 user tokens, and you may be subject to additional terms.

ii. Use the Twitter API as provided by Twitter for functionalities in your Service that are substantially similar to a Twitter service feature and present this to your users as the default option.

iii. Display a prominent link or button in your Service that directs new users to Twitter's sign-up functionality.

Do not do the following:

1. Pay, or offer to pay, third parties for distribution. This includes offering compensation for downloads (other than transactional fees) or other mechanisms of traffic acquisition.
2. Arrange for your Service to be pre-installed on any device, promoted as a "zero-rated" service, or marketed as part of a specialized data plan.
3. Use Twitter Content or other data collected from users to create or maintain a separate status update or social network database or service.

8. Engage in Appropriate Commercial Use

a. Advertising Around Twitter Content

i. You may advertise around and on sites that display Tweets, but you may not place any advertisements within the Twitter timeline on your Service other than Twitter Ads.

ii. Your advertisements cannot resemble or reasonably be confused by users as a Tweet.

iii. You may advertise in close proximity to the Twitter timeline (e.g., banner ads above or below timeline), but there must be a clear separation between Twitter content and your advertisements.

b. Compensation

i. When Content is the primary basis of an advertising or sponsorship sale you make, you must compensate Twitter, recoupable against any fees payment to Twitter for data licensing.

ii. Twitter reserves the right to serve advertising via its APIs ("Twitter Ads"). If you decide to serve Twitter Ads once we start delivering them, we will share a portion of advertising revenue with you in accordance with the relevant terms and conditions.

II. Rules for Specific Twitter Products or Features

1. Twitter Login

a. Present users with easy to find options to log into and out of Twitter, for example, via the OAuth protocol or Twitter Kit.
b. Provide users without a Twitter account the opportunity to create a new Twitter account.
c. 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 your Service.
d. Obtain consent before accessing users' email addresses using Twitter login. As part of Twitter's OAuth protocol, users may consent to share their email addresses with you. On iOS and Android, you must only request access to users' email addresses using the Twitter-approved user interface made available via Twitter Kit and must only access email addresses of users who provide consent through that user interface.

2. Social Updates

a. If you allow users to create social updates from your own social service or a third party social networking, micro-blogging, or status update provider integrated into your Service ("Update"), you must display a prominent option to publish that content to Twitter.
b. If Updates are longer than 140 characters or not text, you must display a prominent link to publish that content to Twitter and:

i. URLs must direct users to the page where that content is displayed. You may require users to sign in to access that page, but the content must not otherwise be restricted from being viewed.

ii. URLs must not direct users to interstitial or intermediate pages.

3. Twitter Identity

a. Once a user has authenticated via Connect with Twitter via your Service, you must clearly display the user's Twitter identity via your Service. Twitter identity includes visible display of the user's avatar, Twitter user name and the Twitter bird mark.
b. Displays of the user's followers on your Service must clearly show that the relationship is associated with the Twitter Service.

4. Twitter Cards

a. Develop your Card to have the same quality experience across all platforms where Cards are displayed.
b. If your Service provides a logged-in experience, the experience prior to a user's login must be of equivalent quality and user value.
c. Mark your Card as 'true' for sensitive media if such media can be displayed.
d. Use HTTPS for hosting all assets within your Card.
e. For video and audio content:

i. Default to 'sound off' for videos that automatically play content.

ii. Include stop or pause controls.

f. Do not do any of the following:

i. Exceed or circumvent Twitter's limitations placed on any Cards, including the Card's intended use.

ii. Attach the App Card to a user's Tweet, unless the user is explicitly promoting or referring to the app in the Tweet.

iii. Place third-party sponsored content within Cards without Twitter's prior approval.

iv. Include content or actions within your Card that are not contextually relevant to the user's Tweet text and Tweet entities, such as URLs and media.

v. Generate active mixed content browser warnings.

vi. Attach monetary incentives or transactions (including virtual currency) to activities that occur within the Card or on Twitter from your Card.

vii. Apply for Cards access for domains you do not manage to prevent others from registering or utilizing Cards on those domains.

5. Twitter for Websites

a. If you expect your embedded Tweets and embedded timelines to exceed 10 million daily impressions, you must contact us about your Twitter API access, as you may be subject to additional terms.
b. If you use TFW widgets, you must ensure that an end user is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the end user's device where providing such information and obtaining such consent is required by law.
c. If you operate a Service targeted to children under 13, you must opt out of tailoring Twitter in any Twitter for Websites button, embedded Tweet, or embedded timeline on your Service by setting the opt-out parameter to be true.

6. Definitions

a. Content – Tweets, Tweet IDs, Twitter end user profile information, and any other data and information made available to you through the Twitter API or by any other means authorized by Twitter, and any copies and derivative works thereof.
b. Developer Site – Twitter's developer site located at https://dev.twitter.com.
c. Tweet – A public posting with a text body of no more than 140 characters made by any end user of the Twitter Service.
d. Tweet ID – A unique identification number generated for each Tweet.
e. Twitter API – The Twitter Application Programming Interface ("API") and the related documentation, data, code, and other materials provided by Twitter with the API, as updated from time to time, including without limitation through the Developer Site.
f. Twitter Marks – The Twitter name, or logos that Twitter makes available to you, including via the Developer Site.
g. User ID — Unique identification numbers generated for each User that do not contain any personally identifiable information such as Twitter usernames or users' names.

Foursquare[42]

FOURSQUARE LABS, INC. API AND DATA LICENSE AGREEMENT

This API and Data License Agreement ("Agreement") applies to your access to, and use of, the content, documentation, code, data and related materials made available by Foursquare Labs, Inc. ("Foursquare") to you (collectively, the "Content"), including through the use of the Foursquare application programming interface (the "API", together with Content, "Foursquare Materials"). By using any Foursquare Materials you agree to this Agreement.

[42] https://foursquare.com/legal/api/licenseagreement

1. WHO CAN USE FOURSQUARE MATERIALS - When you use the Foursquare Materials, you agree to form a binding contract with Foursquare, and follow this Agreement, the Foursquare Platform Policy and all applicable laws. If you're using the Foursquare Materials on behalf of a company, organization, or other entity, then you and that entity (collectively "Licensee"), represent and warrant that you're authorized to grant all permissions and licenses provided in these terms and bind the entity to these terms, and that you agree to these terms on the entity's behalf. Some of the Foursquare Materials may be code that you incorporate into Licensee's applications, products and services ("Licensee Service") that enable functionality. You agree that we may automatically update those Foursquare Materials, and this Agreement will apply to such updates.

2. GRANT OF LICENSE - Subject to Licensee's full compliance with all of the terms and conditions of this Agreement and the Platform Policy, Foursquare grants Licensee a non-exclusive, revocable, nonsublicensable, nontransferable license to download and use the Foursquare Materials to (i) develop, implement and integrate with the Licensee Service and (ii) use, reproduce, distribute, transmit, display and perform the Foursquare Materials as part of the Licensee Service. Licensee may not install or use the Foursquare Materials for any other purpose without Foursquare's prior written consent. Licensee shall not use the Foursquare Materials in connection with or to promote any products, services, or materials that constitute, promote or are used primarily for the purpose of dealing in: spyware, adware, or other malicious programs or code, counterfeit goods, items subject to U.S. embargo, unsolicited mass distribution of email ("spam"), multi-level marketing proposals, hate materials, hacking/surveillance/interception/descrambling equipment, libelous, defamatory, obscene, pornographic, abusive or otherwise offensive content, prostitution, body parts and bodily fluids, stolen products and items used for theft, fireworks, explosives, and hazardous materials, government IDs, police items, gambling, professional services regulated by state licensing regimes, non-transferable items such as airline tickets or event tickets, weapons and accessories, automatic or autonomous control of vehicles, aircraft or other mechanical devices, dispatch or fleet management, or emergency or life-saving purposes. For Licensee Services that provide real-time route guidance, Licensee must have an end user license agreement that includes the following notice: YOUR USE OF THIS APPLICATION IS AT YOUR SOLE RISK. LOCATION DATA MAY NOT BE ACCURATE.

3. PROPRIETARY RIGHTS - As between Foursquare and Licensee, the Foursquare Materials, including any and all Content made available, collected and/or derived through the API (including, without limitation, user data received from the API or submitted to the API), and all intellectual property rights in and to all of the foregoing, are and shall at all times remain the sole and exclusive property of Foursquare and are protected by applicable intellectual property laws and treaties.

4. OTHER RESTRICTIONS - Except as expressly and unambiguously authorized under this Agreement, Licensee may not (i) copy, rent, lease, sell, transfer, assign, sublicense, disassemble, reverse engineer or decompile (except to the limited extent expressly authorized by applicable statutory law), modify or alter any part of the Foursquare Materials; (ii) otherwise use the Foursquare Materials on behalf of any third party; or (iii) design or permit the Licensee Service to disable, override or otherwise interfere with any Foursquare-implemented communications to end users, consent panels, user settings, alerts, warnings or the like, including but not limited to those intended to notify the end user that his or her user data or location data is being collected or used, or intended to obtain consent for such collection or use. Foursquare expressly reserves the right to limit the number and/or frequency of API requests in its sole discretion.

5. MODIFICATIONS TO THIS AGREEMENT. Foursquare reserves the right, in its sole discretion to modify this Agreement and/or the Foursquare Platform Policy at any time by posting a notice to developer.foursquare.com. You shall be responsible for reviewing and becoming familiar with any such modification. Such modifications are effective upon first posting or notification and use of the Foursquare Materials by Licensee following any such notification constitutes Licensee's acceptance of the terms and conditions of this Agreement as modified.

6. WARRANTY DISCLAIMER - THE FOURSQUARE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, FOURSQUARE AND ITS VENDORS EACH DISCLAIM ALL WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, REGARDING THE FOURSQUARE MATERIALS, INCLUDING WITHOUT LIMITATION ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, ACCURACY, RESULTS OF USE, RELIABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, INTERFERENCE WITH QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS. FURTHER, FOURSQUARE DISCLAIMS ANY WARRANTY THAT LICENSEE'S USE OF THE FOURSQUARE MATERIALS WILL BE UNINTERRUPTED OR ERROR FREE.

7. SUPPORT AND UPGRADES - This Agreement does not entitle Licensee to any support for the Foursquare Materials, unless Licensee makes separate arrangements with Foursquare and pays all fees associated with such support. Any such support provided by Foursquare shall be subject to the terms of this Agreement as modified by the associated support agreement.

8. LIABILITY LIMITATION - REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, AND EXCEPT FOR BODILY INJURY, IN NO EVENT WILL FOURSQUARE OR ITS

VENDORS, BE LIABLE TO LICENSEE OR TO ANY THIRD PARTY UNDER ANY TORT, CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR (A) ANY LOST PROFITS, LOST OR CORRUPTED DATA, COMPUTER FAILURE OR MALFUNCTION, INTERRUPTION OF BUSINESS, OR OTHER SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE FOURSQUARE MATERIALS OR (B) ANY DAMAGES, IN THE AGGREGATE, IN EXCESS OF FIVE HUNDRED DOLLARS ($500.00), EVEN IF FOURSQUARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES AND WHETHER OR NOT SUCH LOSS OR DAMAGES ARE FORESEEABLE. ANY CLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT MUST BE BROUGHT WITHIN ONE (1) YEAR AFTER THE OCCURRENCE OF THE EVENT GIVING RISE TO SUCH CLAIM. IN ADDITION, FOURSQUARE DISCLAIMS ALL LIABILITY OF ANY KIND OF FOURSQUARE'S VENDORS.

9. INDEMNITY - Licensee agrees that Foursquare shall have no liability whatsoever for any use Licensee makes of the Foursquare Materials. Licensee shall indemnify and hold harmless Foursquare from any and all claims, damages, liabilities, costs and fees (including reasonable attorneys' fees) arising from Licensee's use of the Foursquare Materials.

10. TERM AND TERMINATION - This Agreement shall continue until terminated as set forth in this Section. Either party may terminate this Agreement at any time, for any reason, or for no reason including, but not limited to, if Licensee violates any provision of this Agreement. Any termination of this Agreement shall also terminate the license granted hereunder. Upon termination of this Agreement for any reason, Licensee shall cease using, destroy and remove from all computers, hard drives, networks, and other storage media all copies of the Foursquare Materials (including all user data), and shall so certify to Foursquare that such actions have occurred. Foursquare shall have the right to inspect and audit Licensee's facilities to confirm the foregoing. Sections 8 through 13 and all accrued rights to payment shall survive termination of this Agreement.

11. GOVERNMENT USE - If Licensee is part of an agency, department, or other entity of the United States Government ("Government"), the use, duplication, reproduction, release, modification, disclosure or transfer of the Foursquare Materials are restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. The Foursquare Materials are a "commercial item," "commercial computer software" and "commercial computer software documentation." In accordance with such provisions, any use of the Foursquare Materials by the Government shall be governed solely by the terms of this Agreement.

12. EXPORT CONTROLS - Licensee shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and Licensee shall not export, or allow the export or re-export of the Foursquare Materials in violation of any such restrictions, laws or regulations. By downloading or using the Foursquare Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any restricted country.

13. MISCELLANEOUS - Unless the parties have entered into a written amendment to this agreement that is signed by both parties regarding the Foursquare Materials, this Agreement and the Foursquare Platform Policy constitute the entire agreement between Licensee and Foursquare pertaining to the subject matter hereof, and supersedes any and all written or oral agreements with respect to such subject matter. This Agreement, and any disputes arising from or relating to the interpretation thereof, shall be governed by and construed under New York law as such law applies to agreements between New York residents entered into and to be performed within New York by two residents thereof and without reference to its conflict of laws principles or the United Nations Conventions for the International Sale of Goods. Except to the extent otherwise determined by Foursquare, any action or proceeding arising from or relating to this Agreement must be brought in a federal court in the Southern District of New York or in state court in New York County, New York, and each party irrevocably submits to the jurisdiction and venue of any such court in any such action or proceeding. The prevailing party in any action arising out of this Agreement shall be entitled to an award of its costs and attorneys' fees. This Agreement may be amended only by a writing executed by Foursquare. If any provision of this Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable. The failure of Foursquare to act with respect to a breach of this Agreement by Licensee or others does not constitute a waiver and shall not limit Foursquare's rights with respect to such breach or any subsequent breaches. This Agreement is personal to Licensee and may not be assigned or transferred for any reason whatsoever (including, without limitation, by operation of law, merger, reorganization, or as a result of an acquisition or change of control involving Licensee) without Foursquare's prior written consent and any action or conduct in violation of the foregoing shall be void and without effect. Foursquare expressly reserves the right to assign this Agreement and to delegate any of its obligations hereunder.

Annex II – List of Acronyms

Acronym	Meaning
AER	Active Evacuation Route
AIA	Athens International Airport
ASRS	Anoeta Stadium San Sebastian
CCTV	Closed-Circuit Television (Video Surveillance)
ECHR	European Convention of Human Rights
EOC	Emergency Operation Centre
GDPR	General Data Protection Regulation
ICTs	Information and Communication Technologies
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification System
SoNeMa	Social Networks Manager