DELIVERABLE 2.1
Unity - Legal and Ethical Framework

Revision 1

Due Date: 31 October 2015
Date of submission: 31 October 2015
Lead Beneficiary of this deliverable: University of Dundee

Dissemination Level: PU

Project Title: Unity
Grant Agreement: 653729
Funding Scheme: Research and Innovation action – Safeguarding Secure Society

Duration Time: 36 months
Start date: 01/05/2015

Project funded by the European Commission within the H2020 Framework Programme

Document Summary Information

Authors and Contributors

Initials	Name	Organisation	Role
MO	Megan O'Neill	UoD	WP2 lead
YH	Yvonne Hail	UoD	WP2 researcher
AW	Andrew Wooff	Napier	WP2 co-lead
DJ	Daniel James	Rini	WP5

Revision History

Revision	Date	Who	Comment
0.1	27/10/2015	Babak Akhgar	Comments on document
0.2	28/10/2015	Lindsey Gunby	Comments on document
0.3	28/10/2015	Aleksandar Stojanovski	Comments on document
0.4	29/10/2015	Jarmo Houtsonen	Comments on document
0.5	30/10/2015	Megan O'Neill and Yvonne Hail	Responses to comments and update

Quality Control

Role	Date	Who	Approved/Comment

CONTENTS

1 INTRODUCTION

1.1 BACKGROUND – PROJECT SUMMARY

Regardless of the geographical location and the cultural context, a central role of the police is the protection of citizens. As globalisation becomes an embedded part of contemporary living, policing organisations are increasingly required to operate at transnational, national and local scales. To balance this broadening of scope, there has been a renewed emphasis on the role that the police play within the local community. In particular, in order for policing organisations to deliver effective local policing which meets the demands of communities there needs to be an awareness of the local context in which the police are situated. To facilitate this shared understanding of local needs between citizens and the police, a robust system of communication between the public, the police, external stakeholders and other civic organisations is proposed. Developing a locally informed, constructive and co-operative approach to problem solving and crime prevention lies at the heart of the Unity project.

The Unity vision is to strengthen the connection between the police and the diverse communities they serve to maximise the safety and security of all citizens. Unity will develop existing community policing (CP) tools, procedures and technologies, advancing concepts to ensure that citizens are integrated as part of local community problem solving and partnership working, helping to identify local policing priorities. This will be done by strengthening the connection between the police and the communities they serve via digital technology, helping to maximise the safety and security of all citizens.

This new and sustainable citizen-centred CP model will have community trust and confidence at its heart, with the ability for more accessible two-way flows of information and communication via the development of a social media app, which will allow for a greater understanding of the problems and issues faced by communities. By working with citizens and community stakeholders to arrive at a full understanding of their concerns, targeted interventions and solutions can be agreed to keep local communities safe.

1.2 PURPOSE AND SCOPE

Given the international scope of Unity and its desire to create locally accountable community policing, in part through the development of relevant technology, an understanding of international and national legal and ethical frameworks is important. The purpose and scope of this report is to outline the legal and ethical frameworks which will structure Unity's work to ensure that it operates at all times in a legally and ethically robust way. The main areas to be considered are the collection, processing, storing and sharing of data and the ethical restrictions on our research into community policing and the operation of the proposed technology to prevent harm to potential research participants and technology users.

The legal framework will take into account European as well as national legislation on data protection. Although all EU member states will be obligated to follow EU law in this area, there is the

potential for national legislation to be more restrictive. The inclusion of Macedonia, at present a non-EU state, in this project raises particular issues with regards to any transfer of data into the country. This report will analyse the level of data protection in each participating nation, as well as European law, to arrive at our recommendations for Unity. These recommendations will ensure that Unity is as robust in its data collection, processing, storing and sharing as possible.

An ethical framework is required in order that both researchers and especially the participants taking part in the project can be assured that best practice is being met by the Unity project, thus promoting confidence in the research and ensuring that the findings adhere to the appropriate ethical restrictions. Ethical guidelines are less explicit and uniform than legal requirements, and therefore a wide range of variability is possible across the member states. This report will take the best practice from each partner nation to develop the most robust ethical framework possible. This framework will apply to all aspects of Unity's research as well as to the operation of the technology itself.

1.3 METHODOLOGY

This report is based on several sources of information and represents the findings of both primary and secondary sources. In terms of primary research, a Delphi Review was carried out through questionnaires with legal and ethical experts in Unity's participating member states (up to 10 in each country). These experts were asked to name the key legislation and guidelines which would be relevant for Unity at the national and European levels. In total 41 experts from 6 countries taking part in the project replied to the Delphi Review with their views.

In addition to this primary research, secondary research was conducted by reviewing the available documentation on EU data protection legislation as well as that of the participating member states. Available documentation on ethical guidelines for social science research was also consulted. Section 3.3.8 below lists the relevant national legislation as well as the data protection bodies for each country. This report represents our conclusions based on these various consultations and our review of the documents.

2 DESCRIPTION OF ACTION PROPOSED BY UNITY

The overall aim of the Unity project is to examine best practice in terms of CP and communication across ten European countries. Through rigorous examination of the technology available and the variety of models of CP, recommendations will be made about the process of enhancing communication between the police and local communities, especially those hard to reach communities where there has traditionally been distrust in the police and barriers to communication.

Unity outcomes will be met by delivering three key strategic objectives:

1. **Community Policing Best Practice** – This strategic objective will take into account past and ongoing EU research and EU prevention policies and analyse community policing as an opportunity to use a community to observe their own environment to identify risk and exchange information through a rich end-user focus. CP will be analysed as a system of facilitating information-sharing and trust building, and will include research into the virtual dimensions of CP.

2. **Community Policing Technology** - This strategic objective will encourage communication between the police, partners and the public by making it possible for citizens to identify their own risks, enabling them to immediately report their concerns to the police. The development of communications technology for CP will have a strong user-centred approach, while the active engagement with citizens and community representatives throughout the life of the project will ensure that their perspectives are embedded in the relevant technological design.

3. **Community policing training and awareness** - This strategic objective will ensure that joint training and awareness raising activities, including virtual training, are designed to meet the needs of citizens, their communities and the police – all activities will take into account the needs of diverse communities and protected characteristics.

Unity will provide law enforcement agencies (LEAs) with a new CP model, a shared framework of governance, enabling tools and the technology to support closer cooperation for greater, more effective, efficient and more inclusive CP. The citizen-centred approach of Unity supports the protection, safety, security and well-being of communities, but will also support a more collective, shared ownership of large scale, collective risk. Coordinated by experts and practitioners in CP, Unity seeks new ways of working in which the police and other LEAs will serve as a catalyst for change within communities, helping the latter to become an integral part of the solution, and thereby sharing the ownership and delivery of a sustainable CP model which simultaneously embraces the benefits of technology while meeting diverse community needs.

2.1 UNITY'S RESEARCH

In order to ascertain the needs of citizens and LEAs in community policing, Unity will undertake a series of interrelated rounds of data collection and primary research. This will include methods such as interviews (face-to-face and over the telephone), questionnaires (face-to-face or electronically), focus groups and pilots. Participants in the research will be drawn from local communities, LEAs,

partner agencies as well as experts in various related matters. These methods of data collection will need to be conducted in ethically robust ways and with appropriately secure methods of data storage, processing and analysis.

2.2 UNITY'S TECHNOLOGICAL COMPONENTS

In order to achieve its vision of enhanced channels of communication to facilitate the sharing of policing priorities for local communities, a mobile application will be developed. This will have one iteration for citizens and one for LEAs. The application will also be supported by a communication portal, as well as requisite data storage facilities. These components will be described in more detail here, in order to guide the analysis of the relevant legal and ethical frameworks to support a robust development and operation of these systems. As the technology described below is in the very early stages of development, what is described here is the current vision. The final version of the applications and portals will depend on the needs of our target community groups (both citizens and LEAs), who have yet to be consulted on this in detail. Thus the technology described here be subject to change in the future, but the overall legal and ethical requirements will remain constant.

2.2.1 CITIZEN MOBILE APPLICATION

The citizen mobile application will enable the citizen to view reports and crime data as well as provide a portal for the citizen to provide additional information ('intelligence') to assist in police investigations and local crime and safety interventions. The citizen will be able to view a certain amount of crime data: there will be aggregate textual reports in each area, complete with various aggregations on local statistics such as type of crime and location. The main part of the application will be a map view over which crime incidents are laid so that it is possible to see pertinent data for certain locations near the user as identified through a global positioning system (GPS) or a location search. Users will be able to filter through specific types of crimes or get aggregate numbers based on their location. They will also be able to view individual incidents through the map and any information relating to it that has been made publically available such as the status of the case.

Using the mobile application, citizens will be able to report a crime, anti-social behaviour or safety issue in the local area, pinpoint where it happened and pass on additional data, in the form of text, audio, video or images so that the police or other LEA will receive this additional evidence and support from the community. Depending on the nature of the data and pending further discussion, the evidence may be put into the public database or kept in private storage area. The data will be filtered to a degree to ensure that the information is passed to the relevant officer, or resolved quickly (where appropriate) by the staff monitoring the data systems.

Each user can develop a digital profile which will allow for trust to be built between LEAs and citizens by enabling two-way communications. Some citizens may want to report anonymously and therefore this option will also be provided. The user profile, where created, may contain some personal information, such as name, address, date of birth/age, contact information, medical conditions, etc. However, users will not be required to provide any or all of this information so that users have total control over which information they wish to share with LEAs. The user will be

informed, however, that additional information may help the LEA to act on the intelligence which the user provides.

GPS location tracking should be sent where possible, given the user's consent, to better enable LEAs to act on the intelligence which is shared. The user will be able to change the location of the incident in case they see the incident occur across the street, for example, or do not report it right away. Where GPS is not available, the user will be able to choose their location or the location of the incident from a list of options to allow accurate information to be sent to LEAs.

Users will have the option to opt in to further communications from LEAs as the incident progresses, in order to get more detailed information of what exactly happened and how LEAs are acting on the intelligence provided. This will be essential for communities looking to take an active role in community policing. Users will opt in through the citizen's profile/settings page where they will be able to select their preferred method of communication. The citizen will have a choice to contact in an anonymous or non-anonymous way: users can provide their contact details or, if they wish to remain anonymous, they could be contacted through the application itself.

It will be possible to gather information about open cases where the incident is made public via the mobile application and intelligence from members of the public is required to progress LEA activities. All information provided will be judged for reliability through a filtering system to rank reliability dependent on the source and the information. When a user reports an incident for the first time, it will have to be approved by a moderator or the responder before anything is available to be seen by the public. Trust ratings will play an important role here. There will be a threshold where after a point, automatic approval shall be permitted for repeat users who are deemed a trustworthy source.

2.2.2 LEA MOBILE APPLICATION

The LEA application will be similar to the citizen mobile application with a slightly different view of the incidents. LEAs will have access to the incident status, with the ability to change, publish or moderate the incidents, based on their permission level via the application. This system will grant officers the ability to update the incident and coordinate activity alongside other LEA officers, as well as the reporters of the incident. As such, access to the application on the LEA side will be very secure and officers must login to verify that they are able to help through the correct area of responsibility and security clearance.

The officer view of the maps will have both new and existing open cases shown whereas the citizen application will only include closed and publicised cases. A feature that allows officers to delegate and coordinate resources within and between LEAs will be implemented as part of the application, allowing officers to monitor the situation as it progresses so they are kept informed. All officers working on the case will have access to the same data.

A status indicator will be available to be updated from the LEA application. Officers will have the option to mark the status of an incident from one of a number of predefined classes. The application will behave differently depending on the status class which is selected. For example, if the incident is closed, the only option available will be to contact the reporter and re-open the incident.

A named officer or responder should be identified for each incident to build trust with the reporter. Having a clearly identifiable LEA contact for each incident which is reported will build confidence and enhance collaboration between LEAs and the application users. Local accountability is a key element of many community policing programmes.

2.2.3 PUBLIC COMMUNITY PORTAL

The public community portal will have similar functionality to the mobile citizen application, although accessible as a website rather than as an 'app'. This portal will be able to retrieve and display crime data and reports about a local area, and will allow users to access information about specific incidents. Thus the portal gives not only a broad overview of the community crime and other incident data but will be able to look deeper into the individual events which allow more detailed information, which has been moderated and approved, to be viewed publicly. The portal will have integration with social media platforms such as Facebook and Twitter and users of these sites will be able to comment on certain incidents on the portal, allowing easy integration with citizens' current online activities.

2.2.4 PRIVATE LEA COORDINATION PORTAL

The private LEA portal will have similar functionality to the LEA mobile application, using web-based technologies as a portal into the database. The LEA Coordination Portal will act as an answering point, similar to the LEA application, where reports may be built and actioned. The Visualisation Console of the portal includes maps and an overlay of all open incident reports, as well as aggregated reports of crime and other incident data for ease of use.

2.2.5 DATA DRIVEN ANALYTICS ENGINE

The Data Driven Analytics Engine will take all the information gathered from the mobile applications and the communications portals and correlate information about same incident, identify patterns and generate reports in a way that operators can use to prioritise actions (e.g. the volume of reports per time of crime, a heatmap per geographical location of the reports, risk statistics, etc.). The data collection system will be linked to external data sources for allowing better analysis. Results from data analytics are incorporated into rich visualisation forms, which will display neighbourhood incidents (e.g. maps with locations of events, event relations, etc.), risk assessments and support decision-making and allocation of resources. The Analytics Engine data analysis and visual representation techniques will provide real-time data visualization and interaction.

2.3 IDENTIFICATION OF ISSUES WITHIN UNITY COMPONENTS

The above components of the proposed Unity CP technology raise certain issues in relation to data protection and the ethical treatment of research participants and app users. The main legal and ethical issues involved which may fall under the remint of European and member states legislation and guidelines will be explored here. The following section of the report will describe in more detail what exactly the applicable laws and guidelines are before making recommendations for the work of Unity in these areas.

2.3.1 CITIZEN MOBILE APPLICATION AND COMMUNITY PORTAL

The citizen mobile application and community portals will allow users to communicate with LEAs in an online tool and to provide potentially sensitive and personal information. This could involve sharing images, videos and GPS location information as well as hidden data such as the user's IP address. Users will need to be made aware of the limitations of this service, the extent of data to be collected and the purposes for which this information will used.

In terms of the information made available to citizen users about crime and other incidents in their area, LEAs will need to ensure that only approved information is made public through the mobile application or portal service. It will be important that only fully vetted and authorised LEA staff have access to the upload function of the citizen app and portal.

Similarly, the integration of the social media sites into the public portal will be done in such a way as not to compromise the security of the site and the security of the information shared between citizens and the relevant LEA privately. Social media users will need to be made aware that posting comments or information about local issues and events in the social media platforms is not an anonymous or secure method of communication with an LEA.

2.3.2 LEA MOBILE APPLICATION AND PRIVATE COORDINATION PORTAL

Due to the additional power of the LEA application with advanced privileges, the damage that could be caused with misuse, loss or hacking into the application could be severe. High security will be needed here and network listeners will need to be created. It is essential that only authorised staff have access to the coordination portal and the database of information provided by and on citizen users. In order to be assured of a secure connection to the app and portal, only staff present on-site in LEA offices will be able to logon to the system. No home working use will be allowed.

2.3.3 COLLECTION OF DATA

Data will be collected via the applications through user input for almost all cases except where the user wishes to save certain data for easy future use. Data will be stored on the Unity database, allowing a profile to be built from the user data. It will be stored in objects that may require some additional security whilst sending the data across applicable networks. Data sent across any network will be encrypted to a high standard to prevent unauthorised individuals from accessing the data within the network or listening out for private data.

2.3.4 STORAGE OF COLLECTED DATA

The data will be stored in a database, the method of which is still undetermined but expected to be a document style NoSQL database which will be capable to scale in and across clusters in order to hold and store big data. The security of the database cannot be compromised. Due to the amount of sensitive personal data and data that could cause harm and damages to citizens and LEAs, high level security is essential. Data encryption and database salting are just a few methods that will need to be implemented.

2.3.5 RETRIEVAL OF DATA FROM DATABASE

The portal will receive data from database over a secure connection. Each user will have a set of permissions pertinent to their role within the LEA so that there is no unauthorised access of sensitive information. Users within the LEA application will be restricted to citizen-level permissions until authorised by a superior officer or other relevant senior member of staff. Citizens using the citizen mobile application will only be able to access information which has been made publicly available by the relevant LEA.

3 DATA PROTECTION

Data Protection in the context of the Unity project includes the collection, processing and the conservation of personal data collected via the mobile application, the citizen portal and the related components accessible by LEAs and Unity researchers. This section of the report will explore the relevant data protection legislation in more detail in order to inform the relevant legal framework for Unity's work.

The protection of personal data is aligned to human rights protections, in particular, with Article 8 of the *European Convention on Human Rights* (ECR) and the protection of privacy and private life. Data protection legislation and directives are constructed around the core principle of an individual's (the data subject) rights to privacy as defined by Article 8 of *The European Charter of Fundamental Rights and the Protection of Personal Data*. Within the Article it states that everyone has the right to:

1. The protection of personal data concerning him or her
2. That such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law
3. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

(European Commission 2013: 5)

3.1 DATA PROTECTION: A TIME LINE

The increased need for data protection legislation occurred as a side effect of the development and wide use of new communication technology which is able to store and share the personal data of individuals. In an effort to prevent violations of human rights in terms of the privacy and the security of stored personal data it was deemed pertinent to introduce some form of framework that would protect individuals but at the same time not restrict the free of movement of personal data across Europe. The current European Directive 95/46/EU utilised for data protection is based on the work of the Organisation for Economic Cooperation and Development (OECD) who in 1980 published *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data,* which they claimed could be employed to form standardised legislation at a national level.

The scope of the recommendations was defined as applying to:

> …personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties. (OECD Annex Part 1 1980:1)

The document states that the guidelines provided were intended to be examples of the *minimum standards* which should then be enhanced by the addition of principles related to the protection of privacy and individual liberties. The recommendations from the OECD include principles focused on:

- **Notice**—data subjects should be given notice when their data is being collected;
- **Purpose**—data should only be used for the purpose stated and not for any other purposes;

- **Consent**—data should not be disclosed without the data subject's consent;
- **Security**—collected data should be kept secure from any potential abuses;
- **Disclosure**—data subjects should be informed as to who is collecting their data;
- **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- **Accountability**—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

With regards to the 'free' movement of data across borders, the OECD sets out what it refers to as principles for the 'free flow and legitimate restrictions' (OECD Annex Part 1 1980:3) of data across other member countries. The first of these principles is based on the secure movement of data from one country to another where it states that it is the responsibility of the country exporting the data to ensure that the country receiving the data is operating within both its own data protection legislations and the guidelines described above.

The recommendations also include a reminder to all nation states that when constructing their internal data protection legislation they should be cognisant of the requirements for the continual 'free-flow' of personal data (particularly within EEA countries) and ensure that neither national laws nor policies would '…create obstacles to the trans-border flows of personal data'
(OECD Annex Part 1 1980:4).

However, these were recommendations and resolutions that could *not* be passed into law by the OECD. This resulted in data protection coverage across Europe being somewhat patchy and inconsistent. In an effort to consolidate data protection coverage across Europe and support the free movement of data between EU member states, the Council of Europe in 1981 brought forward their first treaty with the intention of protecting the individual's right to privacy in terms of the flow of personal data across national borders whilst also supporting individual rights to freedom of information. The treaty entitled *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (CETS No.: 108) which became known as Convention 108 came into force in 1985. The purpose of the treaty was to ensure that every individual, no matter their nationality or country of residence had their right to privacy with regards their personal data situated within state law and placed a specific focus on the sharing of personal data across borders.

The Convention highlighted the inconsistencies in data security across nations and therefore sought to develop a framework which could guarantee a basic fundamental approach to maintaining the security and privacy of personal data across all countries. The preamble of the original document states that the purpose of the convention is based on a consideration:

> …that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing…

(Council of Europe 1981:1)

Whilst offering a secure framework with which to work on personal data, the convention at the same time banned the collection or processing on 'sensitive' personal data which it defined as data relating to an individual's 'race, politics, health, religion, sexual life, criminal record etc.'. The

principles contained in the Convention were later expanded by the current EU data protection Directive 95/46/EC, to be discussed next.

3.2 DATA PROTECTION AT THE EUROPEAN LEVEL: THE DIRECTIVE

The most common control utilised in relation to information policy and the processing and free movement of personal data is the Directive 95/46/EC (from now on called 'the Directive'). The Directive sets out a regulatory framework for collecting and using personal data whilst looking to strike a balance between protecting the individual's right to privacy and the free movement of data. The Directive includes the core principles and rules associated with data protection which each of the 28 EU member states have an obligation to achieve and it further mandates that each of the member states sets up an independent state body to manage data protection. There are of course exceptions to the directive such as data that is collected that is deemed to have influence on public security, defence or state security or personal data that is stored in the private realm. This is laid out in the European Data Protection Directive:

European Data Protection Directive 95/46/EC 1995

The reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data. There are two exceptions this; data that concerns public security, defence, or criminal law and data that is held privately by an individual for personal or household activity (Article 3 (2) Household Exemption)

There are a number of important definitions from the directive:

- **Personal data** – any information that can be used to identify an individual, including voice recordings
- **Sensitive data** – is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information on health or sex.
- **Processing** – any operation which is performed on the personal data such as collection, recording, organising, storage, adaption or alteration (coding), retrieval, use or dissemination
- **Data Controller –** the body or person which determines the purpose and means of the processing of personal data
- **Data Subject –** The individual who supplies the data (participant/respondent)

(Handbook on European Data Protection law 2014: 87)

Directive sets out stringent criteria for the processing of personal data which states that processing of any data may only occur when:

- The data have been collected with the full consent of the 'data subject'
- That processing is necessary for the performance of a contract
- That processing is necessary for compliance with a legal obligation to which the controller is subject; or
- That processing is necessary for the compliance with a legal obligation
- That processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party

(Article 7, Directive 95/46/EC)

The directive also sets the criteria for the 'quality of the data collected before it is processed', stating that:

- Personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be adequate, relevant and not excessive, accurate and, where necessary, kept up to date, must not be stored for longer than necessary and solely for the purposes for which they were collected

(Article 6.1 (a), Directive 95/46/EC)

- Special categories of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis.

(Article 8.1, Directive 95/46/EC)

Under Article 6 of the directive 'data subjects' have the following rights over their personal data:

- **Right to obtain information** – the data controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.);
- The data subject's **right of access** to data: every data subject should have the right to obtain from the controller;
- The **right to object** to the processing of data: the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her. He/she should also have the right to object, on request and free of charge, to the processing of personal data;

(Article 6, Directive 95/46/EC)

Section 7, Article 14 (b) of the directive supplements these rights with further protections for the data subject with regards to the passing on of their data to third party organisations

- The **right to be informed** before personal data are disclosed to third parties for the purposes of direct marketing, and be expressly offered the right to object to such disclosures.

(Article 14, Directive 95/46/EC)

Contained within the directive is legislation which also regulates the movement of data both within and outside European Economic Area (EEA) countries. The first principle of the directive states that personal data cannot be transferred to a country that is outside the European Economic Area (EEA) i.e. the USA, until they can make assurance that they have adequate processes in place to protect the rights and freedoms of the data subject. However, there are no restrictions in place for the movement of personal data within the EU (Articles 25/26, Directive 95/46/EC).

The directive is seen as supporting the *European Convention of Human Rights* (ECHR) Article 8 and 'the right to respect for private and family life, home and correspondence' in terms of providing a legal measure which guarantees information privacy on personal data which fundamentally belongs to the individual. In Article 1 of the Directive, it states:

> In accordance with this directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data (Article 1, Directive 95/46/EC).

3.2.1 EU DIRECTIVE 2002/58 PRIVACY AND ELECTRONIC COMMUNICATIONS

In addition to the Directive, a further level of data protection is important for Unity, the EU Directive 2002/58/EC which is specifically focused on protecting the right to privacy and confidentiality for data and information which is transmitted electronically. The 2002 directive specifically focused on traffic data, spam and cookies in terms of security of data, consent and confidentiality. In 2009 this directive was superseded by Directive 2009/136/EC. Governments across Europe were given until May 2011 to implement the Directive into national law, in the **Netherlands** this has resulted in the Telecommunicatiewet (Telecommunications Act 2012) and in **Finland** the Finnish Information Society Code (2015). In the **UK** this was achieved by the introduction of the Privacy and Electronic Communications Regulations (2003).

In terms of the proposed mobile application for Unity, the sections of the various national legislation documents which have been implemented as per the 2002/58 Directive which are most relevant are those which discuss:

- Keeping communications services secure; and
- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

As per the 95/46 EC Directive there is an obligation on service providers to ensure that there are appropriate security safeguards in place to protect individuals' data and privacy.

It is important to also examine national level data protection mechanisms in the EU as Unity will be operating in a number of different member states.

3.3 NATIONAL LEVEL DATA PROTECTION

Current national level data protection legislation is in the main built on the foundations of the EU Directive. This is not to say that the Directive has been each nation's primary data protection framework. Many EU nations had implemented versions of data protection legislation prior to the

Directive with nations states such as **Germany** introducing a form of national data protection legislation in 1970, **Spain** (in 1978), **Finland** (in 1999) and **Macedonia** (in 1994) all including data protection legislation in their national constitutions. The EU Directive 95/46/EC was an attempt to merge the various levels of data protection across Europe and was the first of many European-wide directives which looked to keep up-to-date with the evolving world of technology and its uses in the sharing of personal data.

Although data protection legislation and/or policy was introduced at various stages at the national level, general data protection coverage across Europe is now very much uniform in terms of the collection and processing of personal data. However, from the point of view of Unity, the protocols stipulated in Directive 95/46/EC will cover all participating countries apart from Macedonia, who is not as yet a full member of the EU.

The inclusion of **Macedonia** in the project therefore raises questions as to the transfer of data collected in the project and forwarded to Macedonia. Principle 8 of the Directive states that 'personal data shall not be transferred outside the EEA, unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data' (Article 26/26 Directive 95/46/EC). This will be taken up further in the section on 'Restrictions on the Transfer of Data' below.

In terms of the scope of data protection legislation across Europe, both **Spain** and **Germany** have the most comprehensive data protection legislation. As with all other European nations they have implemented the Directive in national law with some countries supplementing the EU Directive with their own additional legislation.

3.3.1 DEFINITIONS OF PERSONAL DATA

All of the countries taking part in Unity have carried forward the definition of **personal data** from the Directive:

> 'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Article 2 (a) Data Protection Directive 95/46/EC).

There is related legislation in each country regulating the collection, processing and use of personal data. The reference to **processing** of data is also similar in each nation state and includes the storage, coding, analysing and transfer of all personal data.

In relation to **sensitive data**, the countries included in Unity define 'sensitive' data as per Article 8 of the Directive as being data which reveals; '…racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life' (Article 8 data Protection Directive).

3.3.2 NOTIFICATION AND REGISTRATION

Each country has a national regulatory authority that monitors data protection at a national level. Unique national arrangements within this are:

- In **Belgium** the data controller must notify the Commission before the start of any wholly or partially automated processing operation.
- In **Bulgaria** data controllers must register with the national Commission before exporting data and change their status from data controller to data exporter.
- In **Croatia** registration with the local authority is only required if the data controller is processing 'sensitive data'

In relation to the Unity project, the recommendation should be that all researchers from each nation state should check if they notify their relevant agency prior to the processing of data.

3.3.3 CONSENT

The most fundamental condition given in Directive 95/46/EC with regards to the collection and processing of personal data is 'consent'. In "Chapter 1-General Provisions" the Directive defines consent as

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

(Chapter 1 Directive 95/46/EC)

Consent in many countries should also include information on the purposes of processing the data, the parties to whom the data may be transferred, the conditions for transferring the data to third parties, and the rights of the individual (data subject) concerning further processing of their personal data. The data subject should also be given the contact details for the data controller and processors.

Unique national arrangements to consent are:

- **Estonia** data protection legislation requires that all consent is given in a written format, inclusive of an email, and that in the case of a dispute it is presumed that the data subject has not provided consent and it is the data controller who should prove otherwise.

3.3.4 SCOPE OF DATA PROTECTION LEGISLATION

Finland has supplemental national legislation which regulates employee personal data, data concerning credit worthiness and solvency status of individuals and organisations, the rights of individuals to access their medical files and any other official documentation.

3.3.5 DIFFERENCES IN DEFINITION

In **Finland** an IP address is also defined as personal data in terms of its ability to be used to identify an individual.

3.3.6 RESTRICTIONS ON THE TRANSFER OF DATA

The Data Protection Directive includes restrictions on the transfer of personal data across borders with a particular emphasis on data being forwarded to countries outside the EEA. In order to

transfer personal data to countries out of the EEA, the 'data controller' is responsible for ensuring that the destination country has appropriate security and an adequate level of data protection within its own borders.

Unique national arrangements for data transfer are:

- In **Germany** at present (until 2017, more on this below) national data protection legislation does not apply to a 'data controller' who, although based in another country, is collecting or processing German personal data. If that data is then to be transferred outside the EEA, justifications must be given as to why.
- In contrast however, **Finland's** data protection legislation applies to all 'data controllers' processing Finish Personal Data even though they may not be based in Finland.
- In 2012 **Bulgaria** amended its internal regulations surrounding trans-border data flows so that data controllers are now required to justify the transfer (similar to Germany) prior to gaining the Commission's approval for the transfer

3.3.7 SANCTIONS

In 2011, **Spain,** indicating their strength of intention surrounding data protection legislation (DPL), raised both the classification criteria for breaches of the DPL and the financial sanctions for breaches of the DPL through The Sustainable Economy law (2011). The fines were raised as follows:

- minor breach from E900 to E40,000
- serious breaches from E40,000 to E300,000
- very serious breaches from E300,000 to E600,000.

Other nations who also support fines and sanctions for breaches include the **UK** where sanctions post-April 2010 can be upwards of £500,000.

3.3.8 OVERVIEW OF NATIONAL LEGISLATION

Below is a table showing each of the 10 countries involved in the Unity project with a brief description of their Data Protection Legislation:

Country	Data Protection	Amendments	Data Protection Authority
Belgium	Law on privacy Protection in relation to the processing of Personal Data (1992)	Modified in 1998 to implement the Data Protection Directive. Law of 2003 established national regulatory authority Amended in 2014	Commission for the protection of Privacy http://www.privacycommission.be/
Bulgaria	Personal Data Protection Act (came into force on 1st January 2002)	Amended in 2004, 2005, 2006. Last amended in 2014.	Bulgarian Commission for Personal Data Protection http://www.mvr.bg/en/

			shengen/data_protection.htm
Croatia	The Act on Personal Data Protection 2003. The Act regulates the protection of personal data regarding natural persons and the supervision of collecting, processing and use of personal data in the Republic of Croatia.	In 2006 Croatian Parliament adopted amendments to the Personal Data Protection Act (the "Amendments"). The amendments were enacted with a view to further harmonise the Personal Data Protection Act with EU Directive 95/46/EC as regards transfer of personal data to third countries	Croatian Personal Data Protection Agency http://www.azop.hr/
Estonia	The Personal Data Protection Act 2003	Amended 2007 and 2011	The Estonian Data Protection Inspectorate http://www.aki.ee/en/inspectorate
Finland	Personal Data File Act 1988	1999 Amended to the Personal Data Act (Henkilötietolaki 1999/523)	The Finish Data Protection Board http://oikeusministerio.fi/en/index/theministry/neuvottelu-jalautakunnat/thefinnishdataprotectionboard.html
Germany	The Federal Data Protection Act 1977	The Federal Data Protection Act 2001 the Act on the Protection of Privacy in Electronic Communications 2004 the Act on the Protection of Privacy in Working Life, 2004 Amended 2009 Proposals for further amendments 2015	There are 20 different federal and regional supervisory authorities responsible for monitoring the implementation of data protection Examples of sectoral laws include: Telemedia Act (Telemediengesetz), which applies to providers of telemedia services (such as websites).

			Telecommunication Act (Telekommunikationsgesetz), which applies to providers of telecommunication services. Criminal Act (Strafgesetzbuch). Social Security Code I, II; IV, V and X, which regulate the processing of health and other personal data in connection with the provision of medical and social security services
Macedonia	Protection of Personal Data was adopted in 1994	Amendments In January 2002 this Law was amended, in order to enable an appropriate level of personal data protection, The personal Data Protection Act 2005 2014	Directorate for personal data protection http://dzlp.mk/en
Netherlands	Personal Data Protection Act 2001	June 2012, the Telecommunications Act implements the amendments to the Privacy and Electronic Communications Directive In 2015, new provisions on cookies came into force	Dutch Data Protection Authority https://cbpweb.nl/enPages/home.aspx
Spain	Article 18.4 of the 1978 Spanish Constitution states that the law should limit the use of information technology to guarantee personal privacy. On this basis, the protection of personal data is regarded as a constitutional right in Spain.	Organic Law 5/1992 on the regulation of the Automated Processing of Personal Data and widened the scope of personal data protection offered.	Agencia de Protección de Datos http://www.agpd.es/portalwebAGPD/index-ides-idphp.php
UK	Data Protection Act 1984 introduced basic rules of	1987 Access to Personal Files Act	The Information Commissioner (ICO)

	registration for users of data and rights of access to that data for the individuals to which it related.	Superseded by the Data Protection Act 1998 which came into force on 1st March 2000	

3.4 ONGOING AND FUTURE AMENDMENTS TO DATA PROTECTION LEGISLATION

Technological advancements continue, with evermore personal data now being collected, processed and stored online from the use of social media as well as governmental departments. These ongoing changes therefore necessitate the continual evolution of the Data Protection Directive 95/46/EC to ensure that legislation continues to effectively protect the personal data of EU citizens. There are a few forthcoming changes to note:

The General Data Protection Regulation (GDPR) – (prosed date of adoption 2017)
In 2012 at a meeting of the European Council it was decided that further amendments were required to the Data Protection Directive to ensure the protection of personal data. The GDPR will take the form of a regulation rather than a directive, meaning it will become a legal, enforceable act for all 28 EU member states and will amalgamate all pre-existing European data protection. The amendments will include the following changes:

- Expansion of data protection coverage to all non-EU based companies who store or process the personal data of EU citizens
- The introduction of a European Data Protection Board
- A compliance framework which includes monetary fines for non-compliance
- Companies to appoint independent Data Protection Officers (to ensure compliance)
- Change from the Right to be Forgotten (Article 17 2014) to the Right to Erasure (a right to request erasure of personal data on the grounds of non-compliance)
- Individuals will have easier access to their data

In order to ensure the Unity Project maintains compliance with data protection legislation into the future, these incoming changes, where relevant, will need to be incorporated into its operations.

3.5 DATA PROTECTION FINDINGS FROM UNITY QUESTIONNAIRES

Overall the majority of respondents to the Delphi Review when asked about applicable legislation cited the Data Protection Directive 95/46 for both the member state and European level. This was

the most common response and indicates a general compliance with the Directive. Many respondents also discussed Human Rights legislation in relation to data protection.

The main issues raised by respondents were:

- **Collection**: as per the Directive only the minimum necessary information should be collected for the research project
- **Storage** of the data: that the appropriate physical, technical and organisational security must be in place which will prevent unauthorised access or disclosure of personal data. Steps should also be taken to prevent the accidental loss, damage or destruction of the data
- **Anonymisation**: The research data should be anonymised to ensure no identification can be made to particular individuals
- **Analysis**: should not present any major issues
- **Sharing** data across borders: the requirement (as per the Directive)on the part of the data controller to ensure relevant security (especially with **Macedonia** which is outside the EU)
- **Publication** and access to findings: allow participants to access the findings through free publications or through the public portal.

3.6 POTENTIAL ISSUES RELATING TO UNITY'S COMPONENTS

Some of the proposed components of Unity's mobile applications and portals need additional consideration to ensure compliance with data protection. These are:

- **Images –** Images are defined as 'sensitive' personal data in terms of their ability to reveal ethnicity, race, and in some cases religious beliefs. Taking pictures of young people (those under the age of 18) also has data protection issues.
- **Voice Recordings –** although at present there is no specific mention of voice recordings in either the Directive or any national legislation, the definition of personal data as it stands could be interpreted to include voice recordings (such as voicemail).
- **Portable Hand Held Device for LEAs:** should the LEA mobile application and/or the private portal be made available to LEAs on handheld devices, additional security measures will need to be in place to ensure that should the device be lost or stolen that no authorised access to personal data is possible.
- **Crime maps:** Publishing exact household level data on crime maps is generally considered the processing of personal data in the **UK** and is in contravention of the Data Protection Act 1998, if the data used on the map can identify a specific property in a specific road which in turn can be used to identify an individual and/or group of individuals.
- **Crime maps**: The Information Commissioner in the **UK**, the body responsible for the management of data, also suggests that the frequency of the data uploaded to a crime map can also be used to identify individuals, particularly when the data is uploaded in 'real time'. They highlight their argument by citing an example of a rather 'inquisitive' neighbour seeing a police officer visit a local address and for them then to look on the map to discover a specific crime has been committed.
- **Crime maps**: The Unity portals will be integrated with social media platforms such as Facebook and Twitter. The Information Commissioner in the **UK** states that care should be taken when publishing crime maps on these platforms as they could be viewed alongside other sources of publicly available information which in turn can make individuals and situations identifiable.

These findings will be summarised in the recommendations section of this document to follow, after a consideration of research ethics.

4 ETHICAL GUIDELINES

Research ethics are complex and nuanced and require an embedded understanding of the context in which the research occurs. From expanding our knowledge of science and technology to directing future social policy, research built on trust and integrity is required to engage public support with the findings produced and support future decisions in a variety of aspects. Of key importance is producing work which will avoid a potential conflict of interest, cause no harm to participants, be appropriately rigorous, be based on high quality, robust and rigorous research built on a set of governing principles within an appropriate ethical framework.

In contrast to data protection legislation (discussed above), ethical guidelines for social research across Europe are based on the joint development of specific rules and norms within a variety of disciplines which have been created in line with the *European Convention of Human Rights*, Article 8. ECHR Article 8 states that all individuals have the right to privacy in family and family life and that this right is to be protected at all times. Contemporary research ethics are in the main based around the concepts of '…consent, proportionality, necessity and the right to withdraw' (European Commission 2013:3).

There is a clear connection between research ethics and human rights which is highlighted by the *Convention on Human Rights and Biomedicine* (the Oviedo Convention) (1996) which is also known as *The Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine*. The convention has been used to deploy a European wide minimum standard for research ethics (chapter 5) and with regards to consent (chapter 2). In Europe there is a fundamental commitment to protecting the human rights of all individuals based on the *Charter of Fundamental Rights of the European Union* and the *European Convention on Human Rights.* The Charter includes:

- Article 8 Protection of Personal Data:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Studies which have participants who are children or vulnerable populations or involve deceit, for example, will require additional ethical considerations in light of these conventions. Ethical guidelines in research are employed to protect participants from any harm or potential risk, whether intentional or unintentional, which may occur as a result of individuals being involved in the research process.

In the main, research ethics are based on the following core principles:

- **To cause no harm to participants:** this can include physical harm or psychological harm such as distress caused to the participant by taking part in the research. The universally agreed principle of causing no harm includes restricting research on children or vulnerable populations. Causing no harm also includes maintaining a participant's privacy.

- **Voluntary Participation:** that all participants are aware of the research aims and intentions and have freely agreed to take part in the project without the use of coercion. This also includes the right for participants to remove themselves and their data from the project without causing them any negative impact.

- **Informed Consent**: participants involved in research projects have the right to know that they are being researched. Before obtaining information from any participant in the project, a participant consent form outlining the purpose and background of the project must be signed by each participant. The form should also notify each individual that their participation is voluntary, that they can refuse to answer any questions and are free to remove themselves and their data from the project.

- **Factual Accuracy**: Researchers are obliged to clearly indicate when they are using the work of other, to ensure no falsification of data, no misrepresentation of data, no suppression of data or fabrication of data.

- **Anonymity/Confidentiality:** From a social research perspective, confidentiality can be described as the explicit guarantee given to participants by the researcher that the data they collect will be anonymised with all key identifiers removed. In employing a confidential approach to the collection and dissemination of research data, the researcher is able to A) remove any way of identifying a participant's personal identity from their records and B) encourage participants to be more forthright in their answers.

- **Methodological Principles**: all researchers should ensure that robust methodological techniques and principles are employed in the collection and processing of data.

4.1 WHO IS RESPONSIBLE FOR RESEARCH ETHICS?

As stated above social research ethics are not based in law and as such there are no **legal** requirements to follow. However, the guidelines that are available offer researchers **a minimum acceptable standard** to follow in carrying out research. Organisations and institutions who employ and/or initiate research projects are responsible for ensuring that all research is conducted in a manner which is robust, causes no harm and makes it difficult to falsify data. This has created a somewhat complex mix of institutional and organisational guidelines.

4.1.1 NATIONAL ACADEMIC RESEARCH

Institutions across the world have implemented their own ethics processes and committees which are utilised across all disciplines within the institution and promote research based on trust and integrity. These are based on ethical codes of practice instigated by professional associations, research councils, funders and the government and govern a wide range of research- related activity. Examples include The Association for Research Ethics; Economic and Social Research Council (ESRC) and European Network of Research Ethics Committees (EUREC).

4.1.2 UNESCO – CODE OF CONDUCT SOCIAL SCIENCE RESEARCH (2006)

UNESCO have developed a set of 'Ethical Guidelines' to provide a framework which will guide the practice of social research in an attempt to reconcile ethical or legal dilemmas created when conducting '…international, interdisciplinary, comparative and policy relevant social science'(de Guchteneire 2006:1).

4.1.3 THE EUROPEAN CODE OF CONDUCT FOR RESEARCH INTEGRITY (2011)

Published by the European Science Foundation in 2011, this code of conduct defines research ethics as being a governance tool which is applied at all stages of the research process, including the initial decision on 'is this subject worthy of investigation?' in the funding application and continues through to the dissemination of the findings. The document highlights the ever-changing borders and parameters which surround the pursuit of human and scientific knowledge and therefore acknowledges that the policies and guidelines which support research must also be as flexible. They therefore suggest that the code is not to be taken as a replacement for the pre-existing guidelines available at institutional, organisational or national levels but is instead offered as a self-regulatory method which can '…represent a Europe-wide agreement on a set of principles and priorities for the research community.' (European Code of Conduct for Research Integrity 2011: 3).

4.1.4 EUROPEAN COMMISSION ETHICS FOR RESEARCHERS: FACILITATING RESEARCH EXCELLENCE IN FP7 (2013)

The European Commission define ethics as '…the challenge to do what ought to be done" (ibid 2013:10) in the realms of scientific discovery claiming that although the main ethical principles of research appear clear and unambiguous there are still occasions when these safeguards have been ignored and research misconducted is reported. The principles included by the EC are:

- honesty in communication;
- reliability in performing research;
- objectivity;
- impartiality and independence;
- openness and accessibility;
- duty of care;
- fairness in providing references and giving credit; and
- responsibility for the scientists and researchers of the future.

Employing an ethical framework is fundamental to all research projects. Ethical principles whether from an organisational or institutional context influence many of the decisions and processes utilised in conducting research projects, from the focus of the research, to the participants chosen, the methods used to collect data and the dissemination of the findings. By adhering to a clear and uniform framework of behaviours and actions across the research process, the researcher is able to guarantee the integrity and accountability of the project and therefore their findings. However, ethical processes or principles are NOT universal concepts and vary from one nation to another, as well as within nations. It is the primary role of the researcher to identify the relevant guidelines for both the home country and the country where the intended research will take place as researchers will need to be cognisant of the guidelines of both. By complying with the relevant ethical guidelines in the planning, operationalisation and dissemination of research projects, each investigator is

clearly demonstrating that they have met all due obligations in protecting themselves and their participants from harm.

4.2 ETHICS: CONSIDERATIONS FOR UNITY

The European Commission have shown their commitment to research ethics by offering researchers working on their behalf an ethics issues checklist which should fulfil any and all ethical obligations raised within the Unity project and is inclusive of all organisations from all countries.

The guidelines offered by the European Commission are broad but in the main they are based on ensuring:

> …respect for people and human **dignity,** fair distribution of **research benefits** and burden and protecting the **values, rights** and **interests** of the research participant (Horizon 2020 European Commission 2015:7 emphasis in original).

In order to fulfil their ethical obligations under Horizon 2020 guidelines, Unity researchers **must** obtain:

- Institutional/organisational ethical approval;
- Participant informed consent in writing;
- Full disclosure of the project which should include:
    - A full description of the aims, methods and implications of the research including the nature of their participation;
    - An explanation that their participation is completely voluntary and that all participants have a right to withdraw themselves and their data at any point – without consequence
    - An indication of how their data will be used;
- Confidentiality and anonymity.

These requirements and the relevant documentation and guidance to support them are included in the Unity Deliverable 2.5, *Unity Ethics Framework* (submitted on 1/6/2015), and will be monitored by the Unity Ethics Committee (UEC).

4.3 ETHICAL FINDINGS FROM THE UNITY QUESTIONNAIRES

Ethical matters which were returned via the questionnaire focused on the standard ethical requirements of research generally, which have been discussed above. Replies were received regarding standard ethical guidelines around voluntary participation, anonymity and confidentiality. The concept of notifying participants regarding the publication of the findings and how to gain access to them was also put forward in the replies. Some respondents raised questions as to the inclusion of children under the age of 18 in the research as they might be able to download and use the app.

5 RECOMMENDATIONS

The following recommendations for Unity are based on a consideration of the EU Directive 95/46/EC, the incoming changes of the General Data Protection Regulation (GDPR, prosed date of adoption: 2017), the *European Convention on Human Rights* and the guidelines highlighted through the Delphi Review.

5.1 RECOMMENDATIONS FOR UNITY'S RESEARCH

1. All research data collected for Unity should be held in an anonymised format.

2. The partner which collects the data will retain the key for breaking anonymity securely, and will not release this to other partners unless absolutely necessary.

3. All partners in the Unity project will ensure that their data collection and storage systems are highly secure.

4. Should 'cloud storage' systems be used, preference should be given to systems based in the EU to ensure that EU level data protection requirements are followed by the cloud storage host.

5. When sending data from one partner nation to another, only very highly secure systems should be used. This is particularly the case when sending data to and from Macedonia, which is not yet a full member of the EU.

6. All participants in Unity's research will be asked to give informed consent to participate in the project. This consent should be in writing.

7. All participants in Unity's research will be notified about the retention period of their data, the purposes for which their data will be used, their right to withdraw their participation and their data at any time and that their participation is entirely voluntary. This latter point will be a particular issue for LEA participants, who may be asked to participate in research by a superior officer.

8. Children and vulnerable persons should not be included in Unity's research, due to the more complicated processes of obtaining their informed consent.

9. Participants in Unity's research should have access to the findings from this work, such as research publications or briefing papers. These will be made available, subject to any copyright restrictions, on the Unity Project webpage.

5.2 RECOMMENDATIONS FOR UNITY'S MOBILE APPLICATIONS ('APPS') AND PORTALS

1. All data collected through the Unity app and portals are only to be used for the stated purposes.

2. Only data which is absolutely necessary for the functioning of the app and portal are to be collected.

3. All data collected, stored, processed and retrieved by the Unity app, portals, databases and authorised users will be held and transferred through highly secure systems to prevent loss, damage or unauthorised access. These systems should not be based outside the EU unless absolutely necessary.

4. In order to be assured of a secure connection to the app and portal, only staff present on-site in LEA offices will be able to logon to the system. No home working use will be allowed.

5. Users of the app and portal will be made aware of the limitations of these services, the extent of data to be collected (including their IP address), their right to remain anonymous and the purposes for which this information will used.

6. Users of the app and portal will be given the ability to opt out of the collection of personal and sensitive data about him or her, including their IP address. This should be given in a **clear** and **concise** manner suited to the small screen so that users can give their full consent to the data which is collected about them and the reasons why it is being requested. Users should not feel pressured to supply personal or sensitive information that they do not wish to share.

7. Users will be notified of the parties to whom the data may be transferred, the conditions for transferring the data to third parties, and the rights of the individual (data subject) concerning further processing of their personal data.

8. Users should be given the contact details for the data controller and processors and the retention period of their data.

9. Users will have the right to access the personal data held in relation to them in the Unity databases and the right to rectify it, if need be.

10. LEAs should check with their national regulatory authority as to whether they need to register as a data controller/exporter prior to the processing of data. This is especially the case for LEAs in **Belgium, Bulgaria** and **Croatia**.

11. The app and portals will use encryption services to ensure the secure transfer of data from the app and portals to the LEAs and from the LEAs to other partner agencies, either within that country or outside of it.

12. A Privacy Impact Assessment would be good practice for the app and portals.

13. Crime maps must be designed in such a way that no particular home or address can be identified from a crime or other incident reported on it. This includes cases of multiple crimes/events and uploading events in ‘real time’.

14. In addition, linking events in the crime maps to social media platforms (like Facebook and Twitter) will introduce the possibility of cross-linking of information which could render an individual identifiable. This needs to be avoided.

15. Users will have a right to change their mind and withdraw any personal data which is sent.

16. The app and portals should not be used by children or vulnerable persons, and should be designed in such a way so as to discourage their use by these populations if at all possible.

17. Images, voice recordings and video can be classed as personal data and need to be held as securely as other forms of personal data. This is especially the case if the image or voice of an individual who has not consented to using the Unity app or portal is inadvertently captured by a consenting user. In these cases, very careful consideration should be given before these materials are released on the public portal or app.

18. Images and video of children can have particular data protection issues and should be reviewed carefully before being made public.

19. Should the LEA app and private portal be accessible on portable devices (smart phones, tablets, etc.) these need to be equipped with robust security systems to prevent the data being access by unauthorised individuals should the devices be lost or stolen.

20. Publication of a crime or other incident on the public portal and app should be decided on a case-by-case basis to ensure that no person's privacy is violated. All information published about an incident should be anonymised.

6 REFERENCES

Association for Research Ethics http://arec.org.uk/

Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data accessed at http://www.dataprotection.ro/servlet/ViewDocument?id=178 October 2015

De Guchteneire, P. (2006) UNESCO: Code of conduct social science research accessed at http://portal.unesco.org/shs/en/files/6497/10951456011Soc_Sci_Code.pdf/Soc_Sci_Code.pdf October 2015

Economic and Social Research Council (ESRC) http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/

European Code of Conduct for Research Integrity (2011) accessed at http://www.esf.org/fileadmin/Public_documents/Publications/Code_Conduct_ResearchIntegrity.pdf October 2015

European Commission (2013) Ethics for Researchers; facilitating Research Excellence in FP7 accessed at http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf September 2015

European Commission (2015) Guidance How to complete your ethics self-assessment Accessed at http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf October 2015

European Network of Research Ethics Committees (EUREC) http://www.eurecnet.org/index.html

Handbook on European data protection law (2014) European Union Agency for Fundamental Rights, Council of Europe accessed at http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf October 2015

Organisation for Economic Cooperation and Development (OECD) guidelines (1980) Annex to the recommendations of the Council of 23 September 1980 accessed at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm October 2015

Social Research Association (2013) data Protection Act 1998: Guidelines for Social Research accessed at http://the-sra.org.uk/wp-content/uploads/MRS-SRA-DP-Guidelines-updated-April-2013.pdf September 2015

Official Journal of the European Communities (1995) accessed at http://www.idpc.gov.mt/dbfile.aspx/Directive%2095-46%20-%20Part%202.pdf October 2015