**Pulse Information Sheet for Interviews**

*PULSE objectives and impacts*

The overall objective of PULSE is to improve the preparedness and response of Health Services involved in emergency situations, to mitigate the loss of life and improve survival rates among mass casualties. The project aims to develop a platform for European medical support during major emergencies, such as a stadium crush at a large concert or a SARS-like epidemic. The expected results and final impacts from the PULSE project include:

* Improving health services in both preparedness and response stages of major medical incidents leading to more efficient emergency management
* Operational procedures harmonisation
* Efficient learning tool
* Improving cross border cooperation of the medical services
* Training tools with real life simulations
* Enhanced management of the hospital resources
* Improved understanding of public acceptance, legal, ethical and social issues in major public health emergency management

*The PULSE Platform*





*PULSE Platform Architecture*



*PULSE Information Flows*

This section summarises the basic information flows for the PULSE platform, highlighting the personal data collected, by whom, and how it is used, retained, secured, whether it is disclosed to third parties, and how it is deleted.

Personal data collected

* Full name
* Home address
* Email address
* Date of birth
* Birthplace
* Telephone number
* Screen name
* Nickname
* Password

Data collection

Personal data is collected via the Decision Support and Validation Tool (DSVT) and smartphone app, from first responders and casualties. Personal data is collected and stored in order to monitor a person’s health status and to keep track of the first responder’s profile.

Use of personal data

The emergency coordinator uses personal data via the DSVT, and the first responder uses personal data via the smartphone app. Personal data is used in order to perform analysis for decision support and to provide updated contextual information.

Retention of personal data

The logistic tool, the Post Crisis Evaluation Tool (PCET), and the authorisation tool retain personal data. Data is stored in the internal tools repositories. Data is stored until it is explicitly deleted. Data is stored in order to inform internal reasoning on the stored data.

Security of data

The Authorisation tool uses the OAuth2 standard to secure the communication between the PULSE tools. Data is secured in order to avoid unauthorised access to the data managed by the PULSE tools.

Disclosure of data

Data is disclosed via the DSVT and smartphone app to PULSE platform users. It is disclosed via the graphical user interface provided by the DSVT and the smartphone app. It is disclosed when it is necessary to gain an overview of the casualties’ health status and the first responder’s profiles, and to provide support to the decision makers.

Deletion of data

Data is deleted from the logistic tool, the PCET, and the authorisation tool. Data is deleted directly from the repository, when a DELETE request is sent to the tool (this occurs when the information is no longer needed).