SUMMARY

This study is one of the ten area studies within the ACTIF project. It is specific in that it is a **transversal study**, with a potential impact on all of the functional areas covered by the architecture. The document structure reflects the following three phases: assessment of the current situation, analysis of specific cases, conclusions: feedback on the ACTIF architecture and recommendations.

The right to privacy is a fundamental liberty in a democratic society. In France, the right to privacy derives from the principles in the Declaration of the Rights of Man and the Citizen of 1789. The new information and communication technologies, used by Intelligent Transport Systems (ITS), place particular importance on the right to privacy. Indeed, the new technologies make it easier to abuse information of a private nature. The objective is to avoid the "Big Brother" phenomenon, to which public opinion is becoming increasingly sensitive.

The analysis of the target architecture, especially the study of dataflows and databases, identifies data of a personal nature. Thus, the aim of this study is to steer ACTIF's architecture so that it can be integrated into the legal framework relating to the respect of privacy. It was decided to limit the study to the right to privacy, and to ignore issues of "protection of commercial information" and "competition". Nevertheless, they stem from the same concern: the protection of sensitive information.

Based on meetings with the CNIL (Commission Nationale Informatique et Liberté – France's National IT and Freedom Commission), and on a review of the main texts of French, European and world law, the current review identifies the requirements and constraints which stem from the collection, storage and processing of personal data. This method was also used in relation to the use of video-surveillance in public places. It appears that the use of personal data is authorised within a specific framework, and places responsibilities on the owner. Intentionally limited, the list of requirements which must be respected may be stated thus:

- Obligation to declare the creation of a file,
- Obligation to make this file secure,
- Principle of the special nature of data collected for specific use,
- Obligation to control data retention periods in accordance with specified use,
- Right of fairness of the data collection,
- Right of legitimate challenge to the processing of personal data ,
- Right of information on the use of the data processed,
- Right of access and amendment,
- Right to see files disappear after a defined period.

To these rights can be added the strict management required for the processing of personal data which might reveal racial origin, political, philosophical or religious opinions, trade union membership or sexual orientation (what are known as sensitive data).

Phase 2 studies various real cases in the light of these issues. CNIL's doctrine, along with an analysis of legislative and European texts, clearly show the limits to the ways in which such personal data may be used. It should be noted that a legal analysis relies mainly on concrete

technical or functional elements. The actual implementation of a project involving personal information is thus essential for producing a reasoned opinion. Each application must be specifically studied.

Phase 3 firstly recommends that, given the legal constraints and impacts on the architecture, the use of personal data should be **limited to the absolute minimum necessary**. Secondly, the recommendations are classified under 4 headings:

1. Given the specified framework-architecture, the major recommendation is to fulfil 2 requirements: assign a single manager to each file created, and one or more defined uses, compatible with the manager's responsibilities. These two constraints have a significant impact on the architecture, given that the modelling specifies large files, shared by several managers and attached to different uses. This model runs counter to the elementary right to privacy rules.
2. Conscious of the difficulty of understanding legal texts, 4 awareness and information files have been produced:
   Right to privacy: rules to follow
   Procedure for declaring an automated personal information system
   Video-surveillance: rule to follow
   Procedure for declaring a video-surveillance system.
3. Stored personal information is required, by law, to have adequate protection. To this end, the main functions for protecting such files have been specified, and will have to be implemented as required.
4. Finally, the right to privacy is a specific aspect of the notion of Data Security. Contrary to networked information systems exchanging data, an information system processes other types of sensitive data (commercial data, industrial secrets, etc.), which are the target of several other threats to confidentiality, integrity and availability of data and processes. To avoid a loss of trust on the part of the actors resulting in a limitation of their data exchanges (essential condition for the success of the architecture), one of the areas of work should consist of establishing a security "charter", or even a standard, with which the different actors will need to comply in order to conform with the framework architecture. It should be based on a structured analysis of the threats and risks, and will define the measures to be adopted.