

Molinari Legal Consultancy

UNITED ARAB EMIRATES



LEGAL ASPECTS OF INFORMATION TECHNOLOGY

Transborder Data Flow

by Ottavia Molinari

LEGAL ASPECTS OF INFORMATION SECURITY

Transborder Data Flow

Technology today enables government, organizations and companies to collect and store a large number of personal information and if this fact from one side simplifies and develops the modern way of life on the other expose everyone to a potential and hidden threat. One of our actual concerns is which type of exposure we could have if a foreign government department or company or organization would be given access to all our available information. We are aware for instance how sensitive health data gathered by a hospital organization if shared with an insurance company might prevent an individual to enter into an Insurance Policy Agreement. These and other fundamental concepts have been recently discussed during the VENICE DECLARATION convention held last September in Venice where all data protection commissioners convened and agreed on the need to comply with the common data protection principles and standards in the face of the intensification of the transborder of personal data in order to allow citizens worldwide to attain an adequate and more widely share of protection internationally¹.

The problem related to *the transborder data flow* across national borders, became a common European issue in 1991 when the Convention of Europe started regulating the "Transborder Flow Data Automatically Processed". The idea of protection over data outside the European Union became very sensitive. Subsequently, the DIRECTIVE 1995/46/EC/, which imposed to all the EU state members to conform their internal legislations to its principles by October 1998, specifically regulated the problem in its Articles 25 and 26 setting out an extensive provision for the transborder of data flows to non-members third countries. The DIRECTIVE provides that personal data which are under going processing or intended for processing after the transfer may be transferred to a third country only if that country can insure "adequate level of protection" (Art. 25). The consideration of different elements as the circumstances surrounding the data, the nature of these, the purpose and duration of process in the operation, the country of origin, the country of final destination and the substantial law and institutional aspects of that country are relevant information for evaluating the adequacy of the level of protection offered. The basilar principles clearly indicate that in lack of protection, third countries would not be allowed to receive the transborder of data. If the system created in the EU can be defined satisfactory assuring compliance by the member states to its principles and creating procedures which impose provision on liabilities, sanctions, remedies, supervisory authorities and notification, the problem arises when third countries want to process sensitive data and marketing data. In order to control the transfer of data, the Directive invites all its members to monitor the third countries that are not offering "*adequate level of protection*" reporting violating situations and to denounce those to the special Commission which should evaluate the level of adequacy to the principles contained in the Directive and eventually enter into negotiation for reassuring the adequacy.

As for the relation between the U.S. and E.U. is concerned, historically in early 1998 the dialogue between the European Commission and the U.S. Department of Commerce started in order to head-off the possibility that data transfers to the US might be blocked following the entry into force in 1998 of the EU's Data Protection DIRECTIVE. The Trans Atlantic Consumer Dialogue (TACD) on November 1999 proposed a provisional agreement known as "DRAFT SAFE HARBOR PRIVACY PRINCIPLES" covering the area of authority of the commerce in general while sectors like financial services, transport, and telecommunication were excluded. In this arrangement, the US set the principles and created the framework to which the US companies and organization should have

¹ 22 Conferenza internazionale sulla privacy e la protezione dei dati personali.Venezia. 28/30 September 2000.

complied. Finally, in July 2000 the European Commission valued that the "SAFE HARBOR" arrangement provides "adequate protection" for personal data transferred from the EU to US.² The US companies interested in participating in this program should only voluntarily adhere to the set of data protection principles in a simple self-regulatory way just sending a private letter³ to the Department of Commerce without any outside independent review or verification of their systems used in practice. This self-certification with the Department of Commerce to adhere to the rules of the "SAFE HARBOR" is creating criticisms and doubts.

The U.S. have created a sort of code of conduct between members and left the effectiveness of the system for transferring and operating data internationally at the good level of adherence practiced by the listed companies ensuring transparency and providing assistance and support to those individuals not familiar with these procedures and receiving an appropriate redress in case of not compliance.

The U.S. Federal Trade Commission, if notified of a violation, has the authority to oblige the company to observe the "Harbor Rules", in extreme cases to cancel the company from the "Safe Harbor" list (as remedies), and may impose heavy fines and require the payment of compensation to individuals (as penalties). However, the Federal Trade Commission is not obliged to pursue the claim and the individual is left to choose between an alternative dispute resolution body and an other independent recourse mechanism to which address the complaint.⁴ In this way, the protection system may appear weak in compared with the EU Directive whereby individuals are granted with judicial remedies and the data protection authorities are obliged to follow up the complaints. It can be observed that the enforcement of the principles DIRECTIVE may not provide a satisfactory procedure for consumers in the event of grievance.

In the event of serious violations of the principles involving the private sector and the "harbor company" contests the charges, the EU authorities still maintain the right to suspend the data transferred until the matter is clarified. However, if this supervisory external control shall prove to be not effective, the EU authorities may revert their decision and consider the "SAFE HARBOR" arrangement as "not adequate".

The future of data protection is still not clear since satisfactory results have been reached only in the EU while in large countries like the U.S., the arrangements created have to be fully tested and their principles have not been codified into law.

The promotion of privacy awareness to consumers through information notices and consent procedures (where a consumer is notified of terms and conditions before the contract is entered into) and the effectiveness of a dispute resolution⁵ shall be fundamental steps in the process of assisting citizens worldwide to protect their right of privacy in this era of global communication network.

2 The "SAFE HARBOR" will be fully up and running by November 2000.

3 It is sufficient that the company declare that its statute provide adequate protection and thus meet the requirements of the Directive as regards transfers of data out of the EU.

4 TACD Statement on U.S. department of Commerce Draft international safe Harbor privacy principles and FAQs. 30 March 2000. <http://www.tacd.org/press-release/state300300.html>

5 Transborder data flow contracts in the wider framework of mechanism for privacy protection on global networks. http://www.oecd.org/dsti/sti/it/secur/prod/e_99-15-final.htm