

## PRACTICAL GUIDE TRANSFER OF PERSONAL DATA ABROAD

*Companies, more of you are outsourcing your computing systems, data bases or call centres. These practices involve obligations that you cannot ignore. Follow this practical guide!*

### ➤ DEFINITION

Neither the European Directive 95/46/EC dated October, 24 1995, nor the French law n° 78-17, amended by the law dated August 6, 2004, on data protection define the notion of “transfer.” Consequently, it is the National Committee on Information Technology and Liberties (“CNIL”) that defines the transfer of personal data as “any data communication, copy or movement through a network, or any communication, copy or movement of these data from a support to another, whatever the type of support, insofar as these data are designed to be transferred in the addressee country.”

The following, for example, are considered as transfer of personal data:

- Centralizing the human resources management’s data base of a multinational group,
- Resorting to a foreign call centre and transferring the corresponding file for canvassing, or
- International systems of maintenance.

### ➤ A REGIME DEPENDING ON THE DESTINATION OF THE TRANSFER

- **Transfer within the European Union or the European Economic Area**

The transfer of personal data on French territory or to Member States of the EU or the EEE is **free**. No specific formalities are required by the CNIL, apart from the formalities that have to be completed before the implementation of the processing of personal data.

- **Transfer out of the European Union or the European Economic Area**

Article 25 of the European Directive and article 68 of the French law on data protection provide that: “The data controller may not transfer personal data to a State that is not a Member of the European Community if this State does not provide a sufficient level of protection for individuals’ privacy, liberties and fundamental rights regarding actual or possible processing of their personal data.”

Subsection 2 of article 68 of French law on data protection specifies that the sufficient nature of the protection provided by the State shall be assessed by taking into account:

- the enacted provisions in this State,
- the security measures applied by the State,
- the specific characteristics of the processing, such as its purposes and duration, as well as
- the nature, origin and destination of the processed data.

The European Commission determines, through an “adequacy decision,” if a State provides a sufficient level of protection.

- *Transfer to a state providing a sufficient level of protection*

The transfer of personal data to a State outside of the EU or the EEE that is considered by the European Commission as providing a sufficient level of protection is **free**. No specific formalities are required by the CNIL, except for the formalities that have to be completed before the implementation of the processing of personal data.

Today, the list of States providing a sufficient level of protection is limited to the following: Switzerland, Canada, and the Isle of Man.

- *Transfer to a state not providing a sufficient level of protection*

The transfer of personal data to a State not providing a sufficient level of protection is in principle **forbidden**, except if expressly authorized by the CNIL, unless provided otherwise.

- *Express authorisations by the CNIL and other exceptions*

Indeed, in the absence of sufficient legal protection, the agreement between parties at the time of transfer guaranteed an adequate level of protection may suffice to allow the transfer. This agreement can be drafted in a contract based on standard European Union contractual clauses, or on the Rules Restricting Companies (REC).

The REC are documents adopted by a group, uniting the entire group of subsidiaries, with the goal of regulating the processing and collection of personal data in the group.

The REC, like contracts dealing with transferring of data, should be reviewed and authorised by the CNIL.

In addition, article 69 of the “Information Technology and Liberties” Law establishes other exceptions. The transfer of personal data to another State outside not providing a sufficient level of protection is possible if the data subject has **expressly consented** to the transfer or if the transfer is **necessary *inter alia*** for the protection of the data subject’s life, the protection of the public interest or the meeting of obligations ensuring the establishment, exercise or defence of legal claims.

The transfer of personal data to a State outside of the EU or the EEE not providing a sufficient level of protection is also possible by a decision of the CNIL or, in case of processing mentioned in sections I or II of article 26 of the French law on data protection (State security and criminal offence processing), by a decree made in the prior opinion of the “Conseil d’Etat,” itself made after a reasoned and published opinion of the CNIL, where the processing guarantees a sufficient level of protection of individuals’ privacy as well as their liberties and fundamental rights.

▪ *Special case: transfer to the United States - Safe Harbor Principles*

Safe Harbor is a process implemented by the United States. Companies located in the US can opt into the process as long as they adhere to several principles protecting personal data and privacy (right of access, of opposition, securing the data, etc).

On July 26, 2000 the European Commission adopted an adequacy decision recognizing that Safe Harbor principles ensured a sufficient and adequate level of protection. Consequently, the transfer of personal data to a company located in the U.S. and adhering

to the Safe Harbor principles is **authorized**. The company adhering to the Safe Harbor principles will however have to complete additional steps so that the personal data relating to the employees of exporting companies are covered by the said process. Moreover, a data controller<sup>1</sup> located in France will have to provide the CNIL with relevant extracts of the Safe Harbor List.

### ➤ SANCTIONS

Illegal transfer of personal data is punished by five years' imprisonment and a fine of 300,000 euros (article 226-22-1 of the French penal code).

---

<sup>1</sup> Pursuant to article 3 of the "Information Technology and Liberties" Law, data controller means, unless expressly designated by legislative or regulatory provisions relating to this processing, a person, public authority, department or any other organisation who determines the purposes and means of the data processing.

*Ichay & Mullenex Avocats is a French law firm focusing on all legal issues related to the new technologies, the green business and the sustainable development in France and abroad. They are considered experts in intellectual property and Internet law, e-commerce, online gaming, data protection. Ichay & Mullenex Avocats also assists its clients on all issues related to financing, mergers & acquisitions, restructuring, etc. and advises them on their litigation and arbitration procedures.*